Principales conclusions de la simulation de rançongiciel par Bishop Fox

Illumio Core empêche les attaques de rançongiciel de se propager en moins de 10 minutes

Mettre fin aux violations dans un monde dynamique et hybride

La transformation numérique et le sprint accéléré vers le cloud ont considérablement élargi la surface d'attaque moderne. Là où le SI étaient traditionnellement un environnement sur site, derrière des clôtures, l'architecture informatique moderne est de plus en plus un mélange hybride de centres de données, de clouds publics, de multi-clouds et de points de terminaison.

Au cours des dernières années, de nouveaux niveaux d'hyperconnectivité ont émergé, car une partie encore plus grande de notre monde est devenue distante et numérique. Les opérations de fabrication sont majoritairement automatisées, un déplacement/séjour à l'hôpital est désormais une expérience numérique presque de bout en bout, et vous pouvez entrer et sortir d'un commerce ou d'une agence bancaire sans interagir avec un seul être humain.

Ce changement a créé un nouvel ensemble substantiel de vecteurs d'attaque et de possibilités pour les cybercriminels.

Mettre à l'épreuve Illumio Core

Pour mesurer l'efficacité d'Illumio Core quand il s'agit de détecter et de répondre à une menace active de rançongiciel, Bishop Fox, leader dans les tests offensifs de sécurité et de pénétration, a simulé une série d'attaques. Chaque test a évalué si l'attaque pouvait être arrêtée, combien de temps cela prendrait, combien d'hôtes ont été infectés et combien de tactiques, techniques et procédures (TTP) ont été exécutées.

L'équipe rouge (les attaquants) a utilisé un ensemble bien établi de TTP provenant des cadres MITRE ATT&CK et PRE-ATT&CK pour tenter d'infecter les hôtes. L'équipe bleue (les défenseurs) a utilisé des technologies de détection et de réponse combinées à la segmentation Zero Trust pour mesurer l'efficacité du confinement des rançongiciels.

Les scénarios d'attaque comprenaient :

- Détection seule
- Détection et segmentation Zero Trust pour intervention en cas d'incident
- La détection et la segmentation Zero Trust, bloquant de manière proactive les ports bien connus utilisés par les rançongiciels
- La détection et la segmentation Zero Trust, mise en œuvre proactive d'une clôture complète autour de l'application

Illumio Core arrête les rançongiciels en quelques minutes

L'émulation de Bishop Fox a prouvé que la segmentation Zero Trust empêche les attaques de se propager en 10 minutes, presque 4 fois plus vite que les capacités de détection et de réponse seules. En outre, le rapport a révélé que :

L'EDR doit être associée à la segmentation Zero Trust pour être plus efficace contre les rançongiciels et autres cyberattaques.

Plus la politique de segmentation Zero Trust et les modes de mise en vigueur sont stricts, plus vite les équipes peuvent détecter et arrêter une attaque en cours.

Illumio Core peut limiter de manière proactive la surface d'attaque, réduisant ainsi le mouvement sur le réseau après une attaque initiale.

Les résultats

Le premier hôte infecté est aussi le dernier grâce à la segmentation proactive Zero Trust

SCÉNARIO 1 — Détection seule

Attaque réussie
Tous les hôtes sont compromis

Ce scénario était dépourvu de toute capacité de segmentation Zero Trust et s'est achevé par un succès total de l'équipe rouge. Ils ont pu exécuter tous les TTP et ont infecté tous les hôtes en 2 heures et 28 minutes.

SCÉNARIO 2 — Détection et segmentation Zero Trust pour réponse à l'incident

Attaque arrêtée : 38 minutes 2 hôtes compromis

Dans ce modèle Illumio était déployé en mode visibilité, fournissant des alertes au système SIEM, qui collectait également des données d'événements à partir d'EDR, Active Directory, Sysmon, etc. À la détection d'activité anormale, l'équipe bleue a déployé une politique de confinement. L'attaque a été arrêtée en 38 minutes.

SCÉNARIO 3 —Détection et segmentation Zero Trust, bloquant de manière proactive les ports bien connus utilisés par les rançongiciels

Attaque arrêtée : 24 minutes 2 hôtes compromis

Dans ce scénario, les ports courants utilisés par les rançongiciels ont été bloqués par Illumio pour réduire le mouvement latéral. L'attaque a été arrêtée après 24 minutes, avec seulement deux hôtes compromis.

SCÉNARIO 4 — La détection et la segmentation Zero Trust ont mis en œuvre de façon proactive une clôture complète autour de l'application

Attaque arrêtée : 10 minutes 1 hôte compromis

Une clôture complète a été mise en place autour de l'application, et il n'y eut aucune propagation du rançongiciel. L'attaque a été arrêtée dans les 10 minutes, confinée dans le premier hôte infecté. Ce résultat a été quatre fois plus rapide que le déploiement réactif.

La différence entre ce qu'un attaquant peut faire en 10 minutes et ce qu'il peut faire en 40 ou 150 minutes est spectaculaire. C'est pourquoi il est essentiel d'associer les stratégies de sécurité, de détection et de réponse par périmètre à la segmentation Zero Trust pour stopper la propagation d'une violation.

En adoptant la mentalité Zero Trust consistant à « supposer une violation » et en déployant la segmentation Zero Trust parallèlement à l'EDR, les entreprises modernes peuvent considérablement améliorer leur protection contre les rançongiciels, ce qui peut faire la différence entre la capacité à fonctionner pendant une cyberattaque et une défaillance majeure de l'activité.

Segmenter pour arrêter la propagation

Lisez le rapport d'évaluation complet de Bishop Fox, Simulation 2022 de scénarios rançongiciel.

En savoir plus sur Illumio Core.

À propos d'Illumio

Illumio, la société de segmentation Zero Trust, empêche les failles de sécurité de se propager au travers d'une surface d'attaque hybride. La plateforme Illumio ZTS visualise tout le trafic entre les charges de travail, les systèmes et Internet, définit automatiquement des stratégies de segmentation granulaire pour contrôler les flux de données et isole les actifs de grande valeur et les systèmes vulnérables, soit de manière proactive, soit en réponse à des attaques actives. Illumio protège les organisations de toutes tailles, des Fortune 100 aux PME, en les aidant à stopper les failles de sécurité et les rançongiciels en quelques minutes et en accélérant les projets de transformation numérique et cloud, de manière à leur permettre d'économiser des millions de dollars occasionnés par l'indisponibilité des applications.