Cyber IA Darktrace : Informations d'identification d'e-mail compromises

Les chefs d'entreprise oublient trop souvent à quel point une boîte de messagerie d'entreprise peut être précieuse lorsqu'elle tombe entre les mauvaises mains. Pourtant, une fois qu'ils ont réussi à y accéder, les attaquants disposent d'un grand nombre de possibilités d'attaques et de points de pivot. La facilité avec laquelle les pirates peuvent accéder à ces systèmes (que ce soit par des campagnes d'hameçonnage, par des attaques par force brute ou par des échanges sur le Dark Web) devrait suffire à s'inquiéter.

Dans de nombreux cas, les attaquants pillent votre boîte de réception de toutes les données de valeur qu'elle contient. Les informations personnelles issues de discussions privées ou de factures peuvent être utilisées à des fins de fraude ou de chantage, tandis que les anciennes conversations par e-mail peuvent renfermer des informations extrêmement confidentielles pour l'entreprise. Listes de clients, documents tarifaires, ou même des feuilles de route et des détails relatifs à la propriété intellectuelle : ce type d'information est bien souvent accessible en quelques recherches seulement.

Dans d'autres situations, les criminels utilisent le compte comme une base de lancement pour les étapes suivantes de leurs attaques. Ils restent discrets, en arrière-plan, et récoltent des renseignements sur des dirigeants ou des partenaires de grande valeur, ils consultent les documents, lisent les conversations et apprennent à se fondre dans le paysage en prévision du moment inévitable où ils vont frapper. En cas de prise de contrôle d'un compte dans la chaîne d'approvisionnement, la capacité de lire une conversation par e-mail à mesure qu'elle se déroule et de proposer une réponse plausible constitue souvent le moyen le plus efficace de réussir une attaque sans attirer les soupçons.

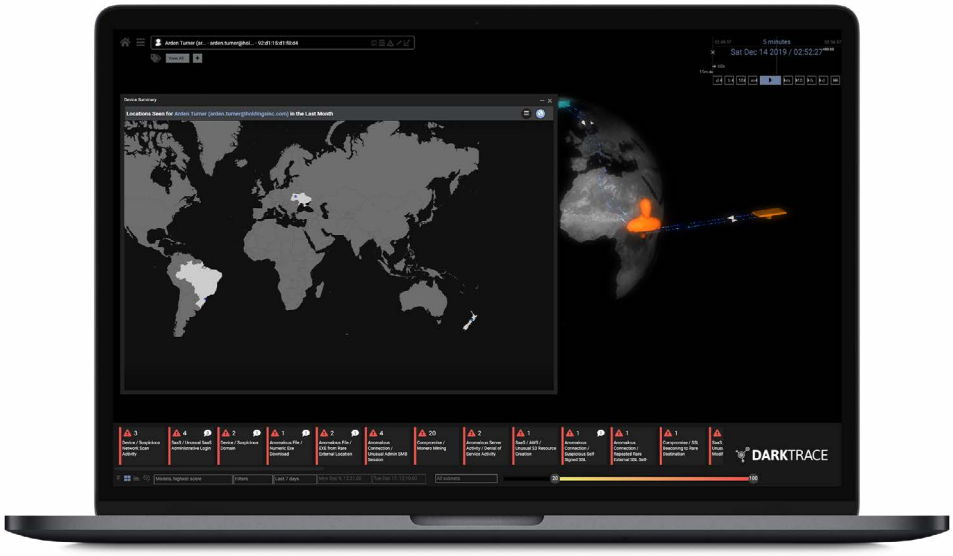

Figure 1: Interface Threat Visualizer de Darktrace affichant l'emplacement géographique de connexion

Performance à l'échelle de l'entreprise

Là où les possibilités sont presque infinies pour les attaquants, les options sont très limitées pour les défenseurs. Les prises de contrôle de comptes professionnels sont en général surveillées par des outils de défense simples et statiques, incluant des règles de « déplacement impossible » qui interceptent rarement les attaquants qui savent se cacher. Cependant, grâce à sa vision de toute l'entreprise, la plateforme Enterprise Immune System de Darktrace complète ces approches basées sur des règles en neutralisant les menaces qui sont inévitablement laissées passer.

À l'instar du système immunitaire humain, Cyber IA de Darktrace utilise des connaissances approfondies de ce qui constitue votre « identité » pour détecter un comportement malveillant qui, sans cela, passerait inaperçu. En apprenant le « modèle comportemental normal » de chaque utilisateur et chaque appareil dans l'entreprise, Darktrace détecte de subtils écarts qui révèlent même les criminels les plus prudents, que ces écarts se manifestent sous forme de comportement de connexion suspect, de création de règles de réception ou de modification des autorisations utilisateur. À l'heure où les cybermenaces gagnent en complexité, faire confiance à une IA auto-apprenante dans l'ensemble de votre entreprise numérique est la seule solution viable pour empêcher les criminels d'accéder à votre système de messagerie.

Étude de cas 1 : Attaque par force brute automatisée

Dans une autre entreprise, Darktrace a détecté plusieurs échecs de connexion à un compte Microsoft 365 utilisant les mêmes informations de connexion, et ce, chaque jour pendant une semaine. Chaque groupe de tentatives de connexion avait lieu précisément à 18h04 pendant 6 jours. La régularité de l'heure et du nombre de tentatives de connexion chaque jour indiquait une attaque par force brute automatisée, programmée pour s'arrêter après un certain nombre d'échecs afin d'éviter tout verrouillage du compte.

Darktrace a estimé que ce modèle de tentatives de connexion était hautement anormal et a alerté l'équipe de sécurité. Si Darktrace n'avait pas corrélé plusieurs indicateurs faibles et ainsi identifié les signaux subtils d'une menace émergente, cette attaque automatisée aurait continué pendant des semaines ou des mois, en tentant de deviner le mot de passe de l'utilisateur en s'appuyant sur d'autres informations récoltées au préalable.

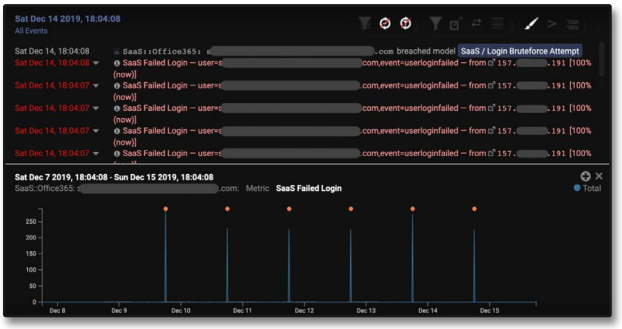

Figure 2: Graphique illustrant les tentatives répétées de connexion

Étude de cas 2 : Compte Microsoft 365 compromis et saboté

Dans une ONG internationale, Darktrace a détecté une prise de contrôle de compte Microsoft 365 qui contournait la règle statique de « déplacement impossible » d'Azure AD. Même si l'organisation possédait des bureaux partout dans le monde, l'IA auto-apprenante de Darktrace a détecté une connexion provenant d'une adresse IP inhabituelle d'un point de vue historique pour cette utilisatrice et son groupe de pairs, et a immédiatement alerté l'équipe de sécurité.

Darktrace a ensuite signalé qu'une nouvelle règle de traitement des e-mails avait été mise en place sur ce compte pour supprimer les e-mails entrants et sortants. Il s'agissait là d'un signe indéniable de compromission, et l'équipe de sécurité a pu verrouiller le compte en question avant que l'assaillant ne puisse causer des dégâts.

Une fois cette nouvelle règle de traitement des e-mails en place, l'attaquant aurait pu lancer de nombreux échanges avec d'autres employés de l'entreprise sans que l'utilisateur légitime ne s'en aperçoive. Cette stratégie est couramment utilisée par les cybercriminels afin de s'installer de façon persistante au sein d'une entreprise, souvent en préparation d'une attaque à grande échelle.

En analysant l'adresse IP rare en conjonction avec le comportement inhabituel de l'utilisateur, Darktrace a identifié avec certitude qu'il s'agissait d'une prise de contrôle de compte et a pu éviter des dégâts sérieux pour l'organisation.