NTT Security

Livre blanc

L'évolution rapide des technologies de déception/diversion

Évaluation des nouvelles techniques de déception dans le cadre d'une stratégie de détection des menaces

Si les RSSI ont beaucoup investi pour tenir les hackers en échec, des attaquants déterminés trouvent encore le moyen de déjouer la sécurité des entreprises.

Alors que leur nombre et leur sophistication ne cessent d'augmenter, les cyberattaques ratissent aussi beaucoup plus large qu'avant.

Quant aux outils de sécurité actuels, ils sont très efficaces pour signaler les anomalies, mais beaucoup moins pour définir leur impact et leur risque potentiel. Résultat : une avalanche d'alertes dont la plupart, bien qu'anodines, doivent être investiguées par les équipes de sécurité. En clair, vos ressources perdent leur temps à évaluer des faux positifs, au risque de laisser passer des menaces bien réelles.

C'est pourquoi de plus en plus d'entreprises s'intéressent aux technologies de diversion ou déception. Selon le cabinet Technavio, ce marché progresse de 9 % chaque année et devrait peser 1,33 milliard de dollars au niveau mondial d'ici 2020. Autrefois l'apanage des pouvoirs publics et des grands établissements bancaires, les technologies de diversion s'étendent désormais à d'autres secteurs. À l'origine de cette expansion, de nouvelles approches sécuritairement plus efficaces et économiquement moins chères à implémenter et à gérer. Toutefois, la course effrénée à l'innovation a semé une certaine confusion quant à l'efficacité, aux fonctionnalités et aux domaines d'application de ces technologies.

D'où la question que tout le monde se pose : l'engouement pour les technologies de déception est-il passager ou marque-t-il une nouvelle étape vers des réseaux résistants à tous types de malwares ?

Qu'est-ce que les technologies de déception ?

Le concept n'a rien de nouveau : même Sun Tzu considérait la supercherie comme le nerf de la guerre. Aujourd'hui, sur le champ de bataille cyber, les équipes de sécurité peuvent créer de fausses cibles afin d'attirer les pirates dans des voies sans issue. Elles maintiennent alors ces leurres sous surveillance, dans l'attente qu'un hacker morde à l'hameçon.

Cette approche permet ainsi de générer uniquement des alertes réseau relativement fiables, puisque toute interaction avec un leurre constitue certainement une anomalie sérieuse. En posant ces pièges à pirates plutôt que de passer au crible des milliers de compromissions potentielles, les analystes en sécurité peuvent se concentrer sur les cas d'infiltration avérés – pratique quand on sait à quel point ils sont débordés.

Outre les honeypots traditionnels, de nouveaux composants factices sont installés sur les serveurs et les terminaux. Par ces nouvelles technologies, les défenseurs musclent clairement leur riposte en réaction à la hausse des cyberattaques. En cas d'échec des défenses périmétriques et des systèmes de prévention, ces pièges permettent de détecter efficacement les intrusions sans effectifs IT supplémentaires.

Ce faisant, les pièges à pirates agissent en renfort des outils de monitoring et d'analyse des comportements d'attaque connus. Ils permettent également aux RSSI de détecter les anomalies du trafic réseau latéral, lorsqu'une intrusion a échappé aux systèmes de détection (cf. Rapport NTT Security récent sur les menaces internes).[1] Le hacker se sert alors d'identifiants usurpés pour parcourir le réseau à la recherche d'informations sensibles.

Bien que la durée moyenne d'implantation des attaquants avoisine les 99 jours,[2] NTT Security est déjà intervenu sur des situations où le réseau avait été infiltré depuis près de six mois.

L'art de la supercherie

Lorsque des professionnels parlent de technologies de déception, ils font généralement allusion aux **honeypots**, une technologie datant de plusieurs

1. NTT Security, Le hacker qui s'ignore Si les salariés mal intentionnés sont les plus médiatisés, la vraie menace interne vient de négligences ou de simples erreurs d'inattention
2. Security Boulevard ; Rapport Mandiant M-Trends 2017

dizaines d'années. Les honeypots, littéralement « pots de miel », désignent de faux serveurs qui, en apparence, font partie intégrante d'un réseau mais n'existe en fait que pour appâter le pirate. Ces logiciels-leurres s'installent sur le serveur, puis se connectent au réseau. Les hackers à la recherche de vulnérabilités les détectent, s'y infiltrent et exécutent leur malware. Les équipes de sécurité reçoivent alors une alerte d'accès au honeypot, puis observent le déroulement de l'attaque. Les hackers peuvent tenter d'installer de nouveaux malwares, ou passent leur chemin s'ils ne parviennent à rien.

Le seul défaut des honeypots, c'est le temps et les efforts nécessaires à leur gestion. Comme n'importe quel serveur, ils doivent être configurés, corrigés et mis à jour. Outre les ressources humaines qu'ils monopolisent, les honeypots peuvent aussi constituer une ligne passive de défense, puisqu'ils attendent patiemment que les attaquants fassent le premier pas. Chaque honeypot doit également faire l'objet d'une surveillance individuelle afin de réagir rapidement en cas d'attaque.

L'autre problème, c'est que les pirates détectent de mieux en mieux la supercherie. Les systèmes informatiques réels génèrent en effet des traces de l'activité de leurs utilisateurs autorisés (fichiers journaux, historiques de navigation, etc.). Les hackers se fient alors à ces traces pour identifier les serveurs et autres systèmes qui méritent leur attention. A contrario, les honeypots ne révèlent généralement aucun signe d'activité, si bien que les attaquants avisés sauront les éviter.

Les traces d'activité servent également aux hackers à se camoufler dans le trafic réseau pour s'y déplacer sans être démasqués. Même une fois infiltrés sur un terminal, ils n'ont pas accès à la topographie globale. Or, les systèmes de protection actuels détectent aisément les recherches de ports visant à localiser des systèmes voisins. Les hackers doivent donc d'abord analyser les systèmes compromis pour identifier leur prochaine cible, puis imiter les comportements du trafic légitime. En dirigeant les attaquants sur de fausses pistes, les RSSI les obligent à passer plus de temps à chercher les informations ciblées, ce qui augmente les chances de détection.

75 % des personnes interrogées citent les pièces jointes d'e-mail comme vecteur des pires attaques subies par leur entreprise, tandis que 46 % mentionnent également les liens contenus dans des e-mails.

Institut SANS, enquête 2017 sur le champ des menaces

Comme d'autres techniques de sécurité, les honeypots se devaient d'évoluer pour devenir l'un des piliers de la sécurité et des procédures de réponse à incident des entreprises. Basés sur le concept de leurre, les **techniques de diversion** de dernière génération appâtent les hackers en créant de faux systèmes déployés sur des équipements bien réels – y compris des serveurs et des ordinateurs portables. Ainsi, les attaquants pensent y trouver des dossiers, des fichiers et des identifiants utilisateurs et administrateurs réels.

Parfois qualifiée de pièges dynamiques, cette catégorie émergente de technologies de sécurité informatique repose souvent sur un mix de leurres régulièrement remplacés ou actualisés pour brouiller encore un peu plus les pistes.

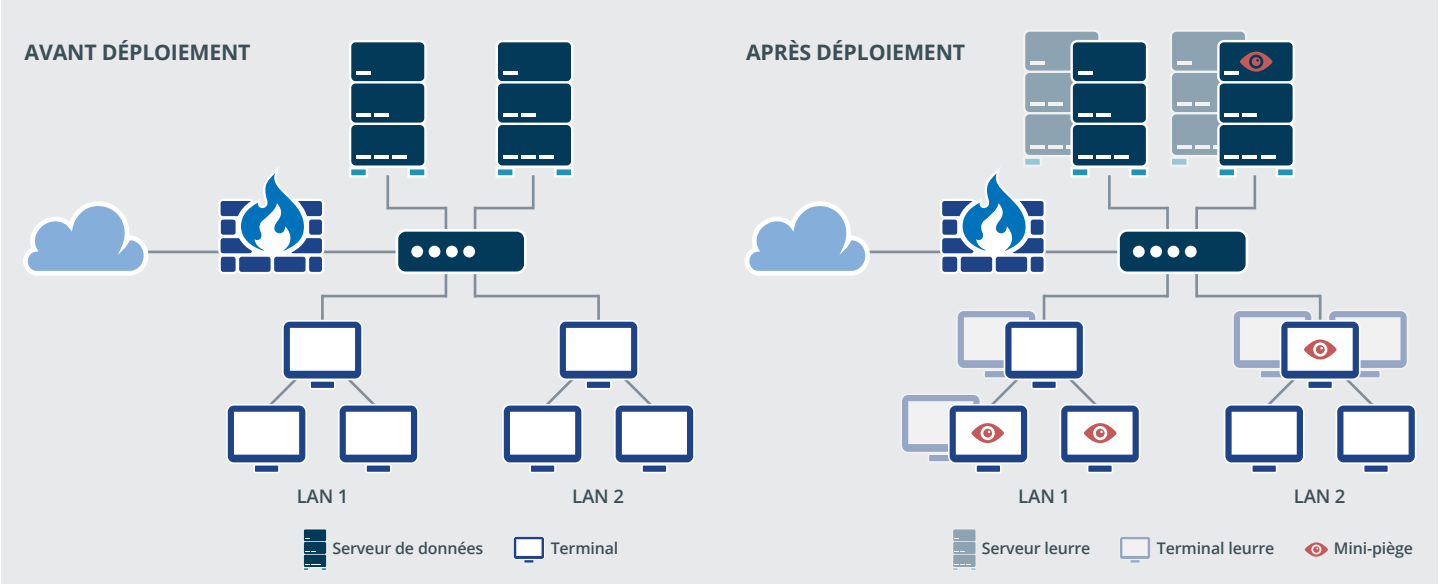
Ces nouvelles technologies de diversion servent essentiellement à lutter contre l'espionnage industriel et le vol de données politiques, scientifiques ou militaires sensibles par d'autres États. Jusqu'ici, ils étaient surtout l'apanage des gouvernements et des entreprises des secteurs de la défense, de l'énergie et de la finance/assurance, tous détenteurs d'informations ultra-sensibles qui les exposent à un feu nourri d'attaques quotidiennes. Toutefois, de plus en plus d'entreprises d'autres secteurs franchissent le pas pour deux grandes raisons : 1) la facilité de déploiement de ces outils et 2) la pénurie d'effectifs qualifiés pour détecter la propagation latérale d'éventuels intrus sur leur réseau.

Mode de fonctionnement

La nouvelle génération de pièges à pirates permet aux équipes de sécurité d'installer des leurres sur leurs terminaux afin d'inonder les attaquants de fausses données (identifiants de comptes utilisateurs mis en cache, historiques de navigation, dossiers partagés, etc.).

La pose de ces pièges s'avère essentielle car, si chaque attaque a ses spécificités, la plupart passent d'abord par les terminaux, notamment ceux des

Schéma 1 : Avant et après le déploiement de technologies de déception. En intégrant des leurres à leur système de défense du réseau, les équipes de sécurité parviennent à identifier la méthode, les technologies et la cible probable des attaquants.



utilisateurs. D'après une enquête 2017 de l'Institut SANS, 75 % des personnes interrogées citent en effet les pièces jointes d'e-mail comme vecteur des pires attaques subies par leur entreprise, tandis que 46 % mentionnent également les liens contenus dans des e-mails.

La proportion de fausses ressources sur un terminal varie, si bien que les hackers ont beaucoup plus de mal à atteindre leur cible et risquent davantage d'être détectés. De fait, chaque action entreprise par un hacker cherchant des données sensibles augmente ses chances de tomber dans un piège.

Une fois sur le leurre, les équipes de sécurité peuvent en apprendre davantage sur l'attaquant et son mode opératoire. Une analyse de malware peut ensuite être effectuée pour assortir automatiquement les alertes d'informations sur les interactions de l'attaquant avec la fausse ressource concernée. Certaines solutions permettent même d'interagir avec l'attaquant pendant une intrusion afin de suivre et comprendre ses méthodes et motivations. Ainsi, les équipes de sécurité peuvent le détourner de sa mission pendant qu'elles identifient sa technique, les technologies utilisées et sa cible probable.

Pour augmenter l'impression d'authenticité, les leurres eux-mêmes sont fabriqués à base d'intelligence artificielle. L'IA analyse les dossiers partagés et les conventions de nommage réseau courantes afin d'imiter les comportements d'utilisateurs bien réels pour créer de fausses pistes.

Toutefois, certains hackers parviennent encore à identifier les leurres et à les marquer comme tels. L'émergence de **pièges adaptatifs** permet heureusement aux équipes de sécurité de repérer ces marquages et d'installer de nouveaux leurres pour piéger les attaquants.

Les entreprises sont prêtes

L'intérêt grandissant des entreprises pour les technologies de diversion s'inscrit dans la tendance plus large d'adoption de services de détection et d'intervention managés (MDR) et d'analytique avancée. Face à la sophistication croissante des attaques et des menaces, les entreprises ont en effet elles-mêmes besoin de hausser leur niveau de jeu pour détecter le trafic latéral suspect sur leur réseau.

Axées sur les menaces réelles plutôt que sur les faux positifs, les informations collectées sur les pièges à pirates peuvent également servir à améliorer les contrôles et diagnostics de sécurité effectués au niveau des pare-feu et autres outils de prévention EDR, IPS/IDS, etc. L'utilisation de leurres sur les terminaux expose instantanément l'attaquant et ses outils, apportant ainsi de précieux renseignements pour réajuster les contrôles de sécurité et prévenir de futures intrusions du même type.

Pour des équipes de sécurité débordées,ces technologies éliminent le besoin d'analyses forensiques et d'investigations approfondies. Ils promettent également d'immuniser les réseaux contre tous types de malwares, recentrant de fait les équipes de sécurité sur la gravité des attaques plutôt que sur le mode opératoire.

Toutefois, les technologies de déception dynamiques ne sont pas faits pour toutes les entreprises. Tout d'abord, il est essentiel de tenir compte du caractère sensible de vos opérations et des partenaires de votre entreprise. Ensuite, pour pouvoir installer des leurres sur vos terminaux, vous devez disposer d'une infrastructure réseau suffisamment avancée.

En somme, les entreprises doivent adopter une approche stratifiée, axée sur la défense en profondeur, afin de mettre en place des contrôles parfaitement réactifs aux spécificités des pièges à pirates et de leur environnement. Contrôle d'accès aux données, installation de correctifs, analyse de fichiers… elles doivent minimiser leur exposition et implémenter des technologies post-intrusion comme ultime rideau défensif contre les attaques les plus avancées.

Conclusion

Pour faire face à la sophistication des cybermenaces actuelles, de plus en plus d'entreprises cherchent des moyens de détection et de neutralisation des intrus infiltrés sur leur réseau. À court terme, la faillibilité des systèmes de prévention ne permettra pas d'apporter des réponses suffisantes.

En rééquilibrant le rapport de force, les technologies de déception/diversion permettent aux équipes de sécurité de se concentrer sur les véritables menaces. Ces solutions doivent toutefois faire partie intégrante d'une architecture de cyberdéfense résiliente. Seule cette approche permettra aux équipes de sécurité de s'appuyer sur les bons processus, technologies et compétences afin de prévoir, prévenir, détecter et neutraliser efficacement la menace.

À l'heure où les pouvoirs publics commencent à imposer ce type de technologies dans certains secteurs comme la banque et le transport maritime, les entreprises ont tout intérêt à abandonner leur stratégie purement défensive au profit d'une approche mixte. L'objectif : inverser les rôles pour prendre les attaquants à leur propre jeu.

L'entreprise NTT Security

NTT Security est la branche et centre d'excellence sécurité du groupe NTT. Nous mettons notre expertise au service des entités du groupe NTT en délivrant des solutions métiers résilientes pour accompagner leurs clients dans leur transformation numérique. Forte de ses 10 centres opérationnels de sécurité (SOC), ses 7 centres de R&D et plus de 1 500 experts en sécurité, NTT Security intervient chaque année sur des centaines de milliers d'incidents à travers six continents.

Pour optimiser l'utilisation de nos ressources locales et libérer le potentiel de nos capacités mondiales, nous offrons un ensemble adapté de services de sécurité managés (MSS) mais également de conseil stratégique ou technologique aux entreprises. NTT Security fait partie intégrante du groupe NTT (Nippon Telegraph and Telephone Corporation), l'une des plus grandes entreprises de TIC au monde. Visitez **www.nttsecurity.com/fr-fr** pour en savoir plus sur NTT Security ou **www.ntt.co.jp/index_e.html** pour le groupe NTT.