Avril 2017

Rapport sur le paysage des menaces

McAfee Labs

Mirai, le botnet de l'Internet des objets

Le botnet Mirai a infecté, puis exploité des équipements IoT mal sécurisés pour lancer la plus importante attaque DDoS jamais connue.

Déroulement de l'attaque

1 Recherche d'équipements IoT
Mirai analyse une large plage d'adresses IP pour rechercher les ports Telnet ou SSH ouverts et localiser les équipements IoT connectés à ces ports.

2 Attaque en force
Mirai lance ensuite une attaque en force contre ces équipements IoT à l'aide d'un dictionnaire de noms d'utilisateur et mots de passe par défaut courants pour identifier les équipements mal sécurisés.

3 Envoi des identifiants
Une fois l'attaque en force réussie, le logiciel malveillant envoie l'adresse IP et les identifiants de l'équipement IoT compromis au serveur de contrôle.

4 Téléchargement du robot Mirai
Un serveur de chargement télécharge le fichier binaire du robot Mirai sur l'équipement IoT.

5 Attente des instructions d'attaque
Une fois l'équipement IoT infecté, le logiciel malveillant attend les instructions de l'attaque DDoS.

6 Lancement de l'attaque DDoS
Mirai est capable de lancer des attaques DDoS sur les couches 3, 4 et 7 du modèle OSI.

2,5 millions
Environ 2,5 millions d'équipements IoT ont été infectés par Mirai.

5 par minute
Toutes les minutes, environ 5 adresses IP sont ajoutées aux botnets Mirai.

1,2 Tbit/s de trafic
Au plus fort de l'attaque, une des cibles du botnet Mirai a été inondée par 1,2 Tbit/s de trafic, le volume de trafic DDoS le plus élevé jamais enregistré.

50 à 7 500 $ par jour
Les attaques DDoS basées sur Mirai sont désormais proposées sous la forme de services à un prix variant entre 50 et 7 500 dollars/jour.

Chronologie de l'évolution de Mirai

1 — *Aux alentours d'août 2016* — **Distribution initiale de Mirai**
Les fichiers binaires ELF de Mirai commencent à faire leur apparition.

2 — *20 septembre 2016* — **Attaque DDoS du site web « Krebs on Security »**
Mirai infecte les enregistreurs numériques et les caméras de surveillance via le port Telnet.

3 — *1er octobre 2016* — **Distribution du code source de Mirai**
Anna-Senpai distribue le code source de Mirai.

4 — *4 octobre 2016* — **Botnet Mirai offert sous la forme d'un service**
Un forum clandestin propose des services DDoS.

5 — *28 novembre 2016* — **Panne du réseau Deutsche Telekom**
Découverte d'une nouvelle variante de Mirai qui cible le port 7547.

Août | Septembre | Octobre | Novembre

Partage de cyberveille sur les menaces

Le danger de l'inconnu

Qu'est-ce que la cyberveille sur les menaces ?

Cyberveille stratégique
Informations traitées et exploitées dans le cadre des activités de planification et de stratégies de sécurité au niveau organisationnel. Celles-ci incluent des éléments comme les auteurs d'attaques et cibles les plus plausibles, les probabilités de risque et les évaluations d'impact, sans oublier les obligations légales et réglementaires.

Cyberveille tactique
Informations collectées par les outils d'analyse, les capteurs et les systèmes de sécurité. Il s'agit souvent d'indicateurs de compromission, particulièrement utiles pour les travaux d'analyse approfondie et les efforts de correction.

Cyberveille opérationnelle
Composants critiques pour l'établissement du contexte. Il s'agit entre autres de déterminer la portée et l'ampleur d'une attaque présumée ainsi que le meilleur moyen de coordonner les mesures correctives. L'analyse des grands volumes de données (Big Data), l'apprentissage automatique et d'autres techniques automatisées de prise de décision sont utilisés dans cette optique afin d'optimiser les capacités et le jugement des techniciens.

Difficultés majeures liées au partage de la cyberveille sur les menaces

Volume
Les capteurs de sécurité, les analyses des Big Data et les outils d'apprentissage automatique génèrent de nombreuses données parasites, dont le volume affecte la capacité à trier, à traiter et à exploiter ces informations.

Validation
Nous devons valider les sources de cyberveille partagées pour garantir que les données proviennent de sources légitimes et non de pirates susceptibles de transmettre des faux rapports pour induire en erreur ou submerger les outils de cyberveille.

Corrélation
Pour mettre en place un plan d'action efficace, il est essentiel de valider les données en temps quasi réel, de les mettre en corrélation sur l'ensemble des systèmes d'exploitation, équipements et réseaux, de trier les événements et d'évaluer l'étendue des mesures nécessaires.

Qualité
Les sources légitimes peuvent par exemple envoyer des indicateurs de compromission à l'ensemble des destinataires de leurs flux d'événements, que ces informations s'avèrent utiles ou non à ces destinataires. Le filtrage, les marqueurs et la déduplication doivent être automatisés afin de rendre la cyberveille réellement exploitable.

Rapidité
Des communications normalisées, ouvertes et en temps quasi réel sont essentielles pour limiter le délai entre la détection d'une attaque et la réception de la cyberveille.

Statistiques sur les menaces

On enregistre 176 nouvelles menaces par minute, soit près de 3 par seconde.

Incidents (974)
Nous avons recensé 197 incidents connus du public au 4e trimestre et 974 pour l'année 2016.

Logiciels malveillants (malware) (24 %)
Le nombre de nouveaux échantillons de logiciels malveillants au 4e trimestre s'élève à 23 millions, en baisse de 17% depuis le 3e trimestre. **Toutefois, dans leur ensemble, les logiciels malveillants ont progressé de 24% en 2016, pour atteindre la barre des 638 millions d'échantillons.**

Logiciels malveillants sur Mac OS (744 %)
Même s'il reste faible en comparaison aux menaces Windows, le nombre de nouveaux échantillons malveillants sur Mac OS a progressé de 245 % au 4e trimestre, une hausse qui s'explique par le parasitage des applications par des logiciels publicitaires. **Le nombre total de logiciels malveillants sur Mac OS a augmenté de 744 % en 2016.**

Logiciels malveillants sur mobiles (99 %)
Le nombre de nouveaux échantillons de logiciels malveillants sur mobiles a baissé de 17 % au 4e trimestre. **Toutefois, leur nombre total a augmenté de 99 % en 2016.**

Réseaux de robots (botnets) de spam (24 %)
Les e-mails de spam émanant des 10 principaux botnets a chuté de 24 % au 4e trimestre, soit 181 millions de messages. Ces dix principaux botnets ont généré 934 millions d'e-mails de spam en 2016.

Logiciels de demande de rançon (ransomware) (88 %)
Le nombre de logiciels de demande de rançon a chuté de 71 % au 4e trimestre, cette baisse étant essentiellement due à une diminution du nombre de détections de ransomware générique, ainsi qu'au déclin des logiciels de demande de rançon Locky et CryptoWall. **Le nombre total d'échantillons de ransomware a augmenté de 88 % en 2016.**

McAfee Global Threat Intelligence

49,6 milliards de requêtes reçues par McAfee GTI en moyenne chaque jour

McAfee GTI

66 millions
Les protections de McAfee GTI contre les URL malveillantes ont **augmenté et atteint 66 millions par jour au 4e trimestre**, contre 57 millions par jour au 3e trimestre.

37 millions
Les protections de McAfee GTI contre les programmes potentiellement indésirables ont **augmenté et atteint 37 millions par jour au 4e trimestre**, contre 32 millions par jour au 3e trimestre.

71 millions
Les protections de McAfee GTI contre les fichiers malveillants ont **diminué et atteint 71 millions par jour au 4e trimestre**, contre 150 millions par jour au 3e trimestre, grâce à un blocage plus important des téléchargements.

35 millions
Les protections de McAfee GTI contre les adresses IP dangereuses ont **augmenté et atteint 35 millions par jour au 4e trimestre**, contre 27 millions par jour au 3e trimestre.

Rapport de McAfee Labs sur le paysage des menaces — Avril 2017

Rendez-vous sur www.mcafee.com/April2017ThreatsReport pour accéder au rapport complet.

Intel Security

© 2017 McAfee, Inc.
2614_0217_info-threat-report-mirai-iot