Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 29 février 2016
N° CERTFR-2016-ACT-009

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-009

1 - Le réseau Tor, une solution d'anonymisation à risques en entreprise

Le projet Tor (initialement l'acronyme de "The Onion Router", ou littéralement "le routeur oignon") est un réseau d'anonymisation qui connaît une popularité croissante ces dernières années. Il propose à l'utilisateur une solution relativement simple à mettre en oeuvre pour éviter que ses communications vers Internet puissent être identifiées, voire surveillées ou bloquées par un tiers (administrateurs réseau, fournisseurs d'accès à Internet ou bien gouvernements répressifs mettant en oeuvre une politique de censure).

Toutefois, bien que plébiscitée pour répondre à des besoins de protection de vie privée sur Internet pour les particuliers, cette solution présente également des limites, en particulier du point de vue de la sécurité pour les entreprises et autres organisations.

Fonctionnement de Tor

Le fonctionnement de Tor repose sur de multiples serveurs, appelés "noeuds", répartis dans différents pays à travers le monde et dont le rôle est de servir de relais pour faire transiter le trafic Internet des utilisateurs.

Ainsi, lorsqu'un utilisateur souhaite établir des connexions sur Internet via le réseau Tor, sa machine va d'abord contacter un serveur capable de fournir une liste de noeuds, ces derniers étant publics. À partir de cette liste, la machine cliente va pouvoir définir un chemin, composé de plusieurs noeuds successifs, sur lequel les données circuleront.

Afin que les communications puissent difficilement être retracées, la connexion entre le client et le noeud d'entrée sur le réseau Tor ainsi qu'entre chaque noeud intermédiaire est chiffrée, et aucun noeud ne connaît l'ensemble du chemin emprunté. Seul le lien entre le noeud de sortie et le serveur destinataire peut ne pas être chiffré : c'est le cas si le trafic relayé via Tor n'est pas censé être sécurisé, par exemple du trafic HTTP. Néanmoins, l'adresse IP de l'utilisateur sera cachée puisque le serveur observera à la place celle du noeud de sortie Tor.

Selon le type de trafic (Web ou messagerie instantanée, par exemple), différents logiciels existent pour se connecter à Tor. Pour naviguer sur le Web via ce réseau, l'utilisateur peut recourir au logiciel "Tor Browser" proposé par les auteurs du projet : il s'agit en fait d'une version du navigateur Mozilla Firefox spécialement paramétrée et à laquelle sont ajoutés des modules complémentaires pour renforcer l'anonymat (Tor Button, HTTPS Everywhere et NoScript). Cette méthode simplifie l'accès à Tor puisque tout le processus consistant à établir un chemin de sortie sur Internet via une succession de noeuds est automatisé et le navigateur est compatible avec les systèmes d'exploitation les plus courants (Windows, OS X et Linux), sans nécessiter d'installation préalable.

Limites et risques de sécurité

Bien qu'ayant été conçu pour répondre à des besoins liés à une utilisation bienveillante, le projet Tor présente des limites dont il faut être conscient pour ne pas négliger certains risques de sécurité.

D'une part, même s'il protège relativement bien ses utilisateurs du suivi des communications et donc leur vie privée sur Internet, Tor n'est pas infaillible. Plusieurs types d'attaque ou faiblesses à différents niveaux ont ainsi pu permettre d'identifier la source des échanges.

D'autre part, Tor peut aussi être utilisé à des fins malveillantes. Outre la navigation sur des sites fréquentés par les cybercriminels et inaccessibles autrement, Tor peut servir à camoufler le trafic réseau de maliciels pour, par exemple, exfiltrer des données sensibles ou créer un canal de communication caché permettant à des attaquants de contrôler des machines infectées. Récemment, le CERT-FR a ainsi informé qu'une campagne de rançongiciels profitait de Tor pour communiquer plus discrètement avec les attaquants (cf. bulletin d'actualité CERTFR-2015-ACT-004).

Enfin, d'autres problèmes peuvent se poser par l'emploi d'un réseau d'anonymisation tel que Tor, et plus particulièrement dans un environnement professionnel ou scolaire. En effet, un utilisateur, dont l'intention n'est d'ailleurs pas forcément malveillante, peut recourir à cette solution pour contourner des mesures de sécurité mises en oeuvre pour limiter les risques de fuites d'informations dans une entreprise, ou l'accès à des contenus inappropriés dans un établissement scolaire.

Recommandations

Compte tenu des risques liés à une solution telle que Tor pour anonymiser du trafic sur Internet, le CERT-FR recommande de détecter voire bloquer les communications qui pourraient être établies vers des noeuds Tor, même si son utilisation n'est pas explicitement proscrite par la PSSI (politique de sécurité du système d'information) de l'organisation.

Parmi les pistes envisageables pour bloquer les connexions Tor, une solution consisterait à mettre en place un serveur mandataire (proxy) pour filtrer les connexions sortantes et ainsi empêcher qu'un client Tor puisse accéder directement à Internet. De plus, des listes de noeuds Tor connus étant disponibles publiquement (cf. Références), les adresses IP correspondantes peuvent aussi être filtrées. À noter toutefois que certains noeuds sont susceptibles d'héberger d'autres services légitimes, qui deviendraient alors inaccessibles.

Par ailleurs, les noeuds Tor utilisent fréquemment les ports 80, 443, 9001 et 9030 : ces deux derniers peuvent donc potentiellement être bloqués au niveau du pare-feu. En ce qui concerne le trafic sur les ports 80 et 443, un filtrage applicatif est nécessaire pour pouvoir différencier les connexions Tor de la navigation Web.

En cas de tentatives de communication observées, il sera alors possible d'identifier la machine à l'origine des requêtes sur le réseau interne, et de vérifier s'il s'agit bien d'une action légitime et maîtrisée par l'utilisateur. De telles investigations pourraient conduire à l'identification d'une machine compromise et utilisée par des attaquants.

Documentation

- Projet Tor :
  https://www.torproject.org
- Bulletin d'actualité CERTA-2007-ACT-047 :
  http://www.cert.ssi.gouv.fr/site/CERTA-2007-ACT-047/CERTA-2007-ACT-047.html
- Bulletin d'actualité CERTA-2010-ACT-008 :
  http://www.cert.ssi.gouv.fr/site/CERTA-2010-ACT-008/CERTA-2010-ACT-008.html
- Bulletin d'actualité CERTFR-2015-ACT-004 :
  http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-004/
- Listes de noeuds Tor :
  https://torstatus.blutmagie.de/ et
  https://www.dan.me.uk/torlist/

2 - Yara, un outil de détection accessible

Avec l'accroissement du nombre de menaces informatiques, il devient nécessaire d'être réactif aussi bien sur le volet de la détection que celui de la prévention et de la réponse. *Yara* est un langage permettant d'écrire simplement des signatures de détection. Ce langage se base sur un ensemble d'artefacts, contenus dans les données à analyser, reliés par des conditions.

Ces artefacts peuvent être des chaînes de caractères, des expressions rationnelles ou des séquences hexadécimales. *Yara* permet ainsi de déployer rapidement des signatures de détection qui permettent d'analyser un ensemble de données (fichier, copie de disques, flux réseau, pages HTML, etc.).

Yara pour la détection

Les signatures *Yara* peuvent permettre de détecter des menaces en avance de phase. En effet, des signatures pour des codes connus peuvent être utilisées pour analyser des fichiers avant leur ouverture ou leur exécution. Cela peut permettre notamment d'effectuer des levées de doute rapidement, notamment sur les pièces jointes des courriers électroniques.

Aussi, dans le cadre d'attaques ciblées, les groupes d'attaquants peuvent notamment envoyer des courriels d'hameçonnage afin d'inciter leurs cibles à cliquer sur des liens malveillants. Dans ce cas, *Yara* pourrait permettre de détecter ces messages frauduleux en recherchant, par exemple, dans les messages échangés la présence de domaines connus pour distribuer des charges malveillantes.

Enfin, *Yara* peut aussi, dans certains cas, permettre de décrire des exploitations de vulnérabilités. Ce cas d'usage permet alors de détecter les fichiers exploitant des vulnérabilités connues lors de leurs arrivées sur une machine ou un réseau.

Yara pour la classification

Dans le cadre de l'analyse de code malveillant, aussi bien pour de la réponse à incident que de la recherche, il est intéressant de pouvoir trier rapidement un grand ensemble de binaires pour identifier ceux déjà connus. Cela permet à l'analyste d'économiser un temps précieux en évitant l'analyse de codes précédemment analysés et éventuellement identifier une menace déjà connue.

Yara dans la recherche de compromission

Lors d'une compromission, les attaquants laissent en général des traces sur le(s) système(s) touché(s). Une bonne partie de ces traces sont des fichiers (courriels harpons, charges malveillantes déposées, etc.) et peuvent donc être recherchées sur d'autres systèmes pour vérifier s'ils sont oui ou non compromis.

Ainsi, dans le cadre d'une analyse *post-mortem*, les signatures peuvent être utilisées pour analyser des copies de disques ou des copies à chaud de la mémoire vive à la recherche de trace de compromissions connues.

Enfin, au-delà d'une unique machine, les signatures *Yara* peuvent être utilisées à l'échelle d'un parc complet à la recherche d'artefacts pour identifier la présence ou non de marqueurs connus sur une ou plusieurs machines.

Outillage

Il existe à l'heure actuelle des outils permettant des analyses avec des signatures Yara. Le principal est celui proposé par les concepteurs. Il s'agit d'un outil en ligne de commande (donc facilement manipulable par des scripts) disponible pour les plateformes Windows, Linux et Mac OS X. Le projet *Yara* propose aussi un module Python permettant d'embarquer dans des scripts du dit langage la possibilité de scanner avec des signatures.

Aussi, d'autres programmes proposent *Yara* en leur sein. On peut notamment citer *Volatility* (extension *yarascan* permettant des recherches dans l'antémémoire), *Loki* (outil de recherche d'indicateurs de compromission acceptant les signatures au format Yara) ou encore *Cuckoo Sandbox* (solution de bac à sable qui peut analyser les fichiers soumis avec Yara).

Documentation

- Page officielle du projet *Yara* :
  https://plusvic.github.io/yara
- Volatility :
  http://www.volatilityfoundation.org/
- Loki :
  https://github.com/Neo23x0/Loki
- Cuckoo Sandbox :
  https://www.cuckoosandbox.org/

3 - Rappel des avis émis

Dans la période du 22 au 28 février 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-069 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu

- CERTFR-2016-AVI-070 : Multiples vulnérabilités dans le noyau Linux d'openSUSE
- CERTFR-2016-AVI-071 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-072 : Multiples vulnérabilités dans Drupal
- CERTFR-2016-AVI-073 : Multiples vulnérabilités dans le noyau Linux de Suse

Gestion détaillée du document

29 février 2016 version initiale.