

Les sites web éphémères, une menace pour les entreprises

Si la grande majorité des sites web temporaires sont mis en place pour générer des activités tout à fait légitimes (comme le partage et la diffusion de contenu), une part non négligeable d'entre eux s'inscrit dans des objectifs plus douteux. C'est sur ces derniers que Blue Coat Systems a concentré son attention dans le cadre d'une étude interne basée sur l'analyse de plus de **660 millions de noms de serveurs uniques** (hostnames) consultés par plus de 75 millions d'utilisateurs dans le monde sur un trimestre (90 jours). Soit un nom de serveur pour 10,6 individus sur Terre. Une quantité suffisamment grande pour être représentative de la réalité.

Il en ressort que **71% d'entre eux ont une durée de vie très éphémère** qui ne dépasse pas les 24 heures. Le spécialiste de sécurité pour les réseaux d'entreprise a ainsi relevé que 22% des 50 principaux domaines couvraient des activités malveillantes comme la gestion de botnets (réseaux de machines infectées et contrôlées à distance). *« Ces sites éphémères peuvent être utilisés pour créer des architectures dynamiques de commande et de contrôle évolutives, difficiles à tracer et simples à mettre en place, remarque l'étude. Ils peuvent également servir à créer un sous-domaine unique pour chaque e-mail de spam afin d'éviter d'être détecté par les filtres anti-spam et les filtres Web. »*

Prendre de vitesse les systèmes de sécurité

Ainsi, de par leur existence limitée, les sites web éphémères sont à même de prendre de vitesse les systèmes de sécurité en échappant à leur vigilance et servir de relais d'actes malveillants. Et leur grand volume complexifie leur recensement permettant à nombre d'entre eux d'échapper aux blocages que les solutions de sécurité appliquent facilement aux domaines statiques. Par exemple, Blue Coat site le domaine «*.1-tr-18su-ka-8dow-56-oo9-13swx-r-k-ife-0nj-rnq-ihb-dd-p-1-0-z-a.info», hébergeant un serveur de commande et contrôle pour un cheval de Troie, qui a généré plus de 1,3 million de sous-domaines sur la période de l'étude. *« La création et la suppression rapides de nouveaux sites inconnus déstabilise beaucoup de systèmes de sécurité actuels »*, reconnaît **Tim van der Horst**, chercheur en chef spécialisé dans les menaces chez Blue Coat.

Pour renforcer leur sécurité, les entreprises doivent donc aujourd'hui s'appuyer sur des systèmes automatisés, temps réel, pour identifier et classer les sites éphémères afin de les empêcher de nuire. C'est notamment la voie suivie par Blue Coat qui, en décembre dernier, [a lancé son offre Advanced Threat Protection](#) (ATP) pour lutter contre les menaces connues et inconnues en s'appuyant notamment sur des technologies de bac-à-sable d'analyse de code avant d'en autoriser l'exécution.

ONE-DAY WONDERS

How Malware Hides Among the Internet's Short-lived Websites



Blue Coat researchers analyzed more than 660 million unique hostnames from a 90-day period.

Researchers found that

71%

or 470 million, were "One-Day Wonders" - hostnames that only appeared for a single 24-hour period.

PROVIDE IDEAL COVER FOR THE BAD GUYS



The sheer volume of One-Day Wonders provide ideal cover for malicious activity, including bot communications with command and control servers.

ONE-DAY WONDERS ARE POPULAR WITH CYBER CRIMINALS BECAUSE THEY:



Keep security solutions guessing with dynamic domains.

Overwhelm security solutions with a high volume of domains.

Hide from security solutions when combined with encryption to deliver malware/steal data.

TOP MALICIOUS DOMAIN



During the 90-day analysis window, the top malicious subdomain:

Ranked 12th on the list of One-day Wonders.

Was a command and control server for a Trojan dialer.

Had more than 1.3 million subdomains.

UNDERSTANDING ONE-DAY WONDERS IS ESSENTIAL FOR BUILDING A BETTER SECURITY POSTURE

Key lessons from this research include:

Static or slow-moving defenses won't protect users and corporate data.

Automated, real-time intelligence is required to separate the noise from the threats.

Identify and assign risk levels to these One-Day Wonders.

Inform policy-based security controls to block malicious attacks.

BLUE COAT

crédit photo © bloomua - shutterstock

Lire également

[Blue Coat va jouer dans le bac-à-sable de Norman Shark](#)

[Blue Coat Systems résume le Byod dans une infographie](#)