VEILLE INFORMATIONNELLE

SPY EYE

L'INTRODUCTION POUR NOTRE VEILLE INFORMATIONNELLE

- ***SpyEye*** *est un malware bancaire de type cheval de Troie bancaire qui a été utilisé principalement pour voler des informations bancaires et des données personnelles sensibles. Développé en 2009, il a été conçu pour infecter des ordinateurs et des appareils, puis collecter des informations relatives à des transactions financières, telles que des identifiants bancaires, des mots de passe, des numéros de cartes de crédit*

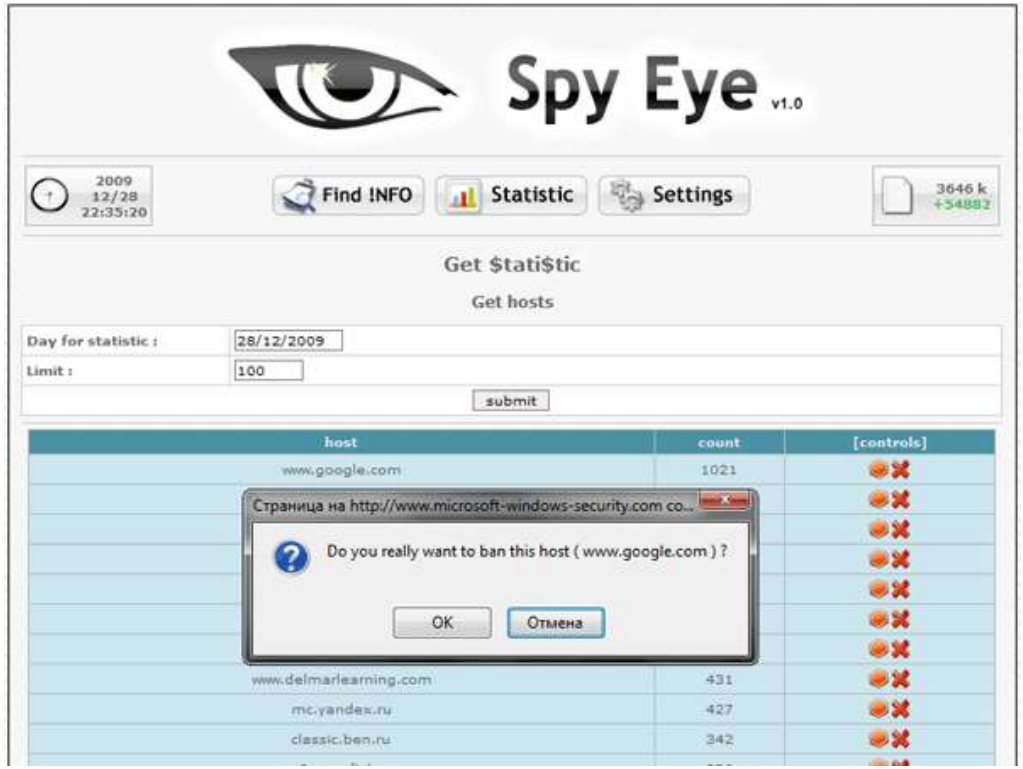
LE FONCTIONNEMENT DE SPY EYE

SpyEye utilise un **keylogger** (registre des frappes) pour enregistrer les touches pressées par l'utilisateur. Lorsqu'un utilisateur saisit des informations bancaires, celles-ci sont envoyées directement au cybercriminel.

Hameçonnage (Phishing) : SpyEye peut afficher des pages Web falsifiées qui imitent celles des banques ou des sites financiers, trompant l'utilisateur pour qu'il saisisse ses informations de connexion.

Botnet : SpyEye permet à l'attaquant de contrôler un réseau d'ordinateurs infectés (un **botnet**) pour effectuer des actions comme l'envoi de spam, la récupération de données, ou encore la réalisation d'attaques DDoS (attaque par déni de service distribué).

Interface de Commande et de Contrôle (C&C) : Les machines infectées par SpyEye communiquent avec un serveur de commande et de contrôle (C&C), qui permet à l'attaquant de gérer et de piloter les actions du malware. Ce serveur C&C est souvent caché derrière des proxys ou des VPN pour masquer son identité



L'IMPACT DE SPY EYE ET LA PRÉVENTION

SpyEye a infecté plusieurs centaines de milliers d'ordinateurs, voire plus d'un million dans le cadre de
Ses attaques. Ça leurs a permis de vol des données bancaires, Fraude par carte bancaires, vol d'identifiants personnels

Quelque méthode de prévention:

Utiliser des outils de détection tel que **VirusTotal** et **TrojanHunter**, qui peuvent analyser les fichiers pour détecter des malwares.

Surveiller les forums de cybercriminalité Les forums de Dark Web et Underground sont des lieux où les attaquants échangent des informations et des outils c'est là ou SPY EYE est commercialisé

Suivre les alertes de sécurité : S'abonner à des bulletins de sécurité comme ceux de US-CERT (United States Computer Emergency Readiness Team) ou d'autres agences comme Europol et Interpol.

Se tenir à jour avec les bases de données de menaces : Comme CVE (Common Vulnérabilités and Exposures) et MITRE ATT&CK, qui fournissent des informations détaillées sur les techniques et vulnérabilités utilisées par les attaquants

RESSOURCE ET BIBLIOGRAPHIE

FireEye Blog une entreprise de cybersécurité renommée, a régulièrement publié des analyses sur SpyEye et des URL : https://www.fireeye.com/blog.html

Kaspersky Securelist est un leader dans l'analyse des malwares et propose régulièrement des articles détaillés sur des menaces telles que SpyEye URL : https://securelist.com/

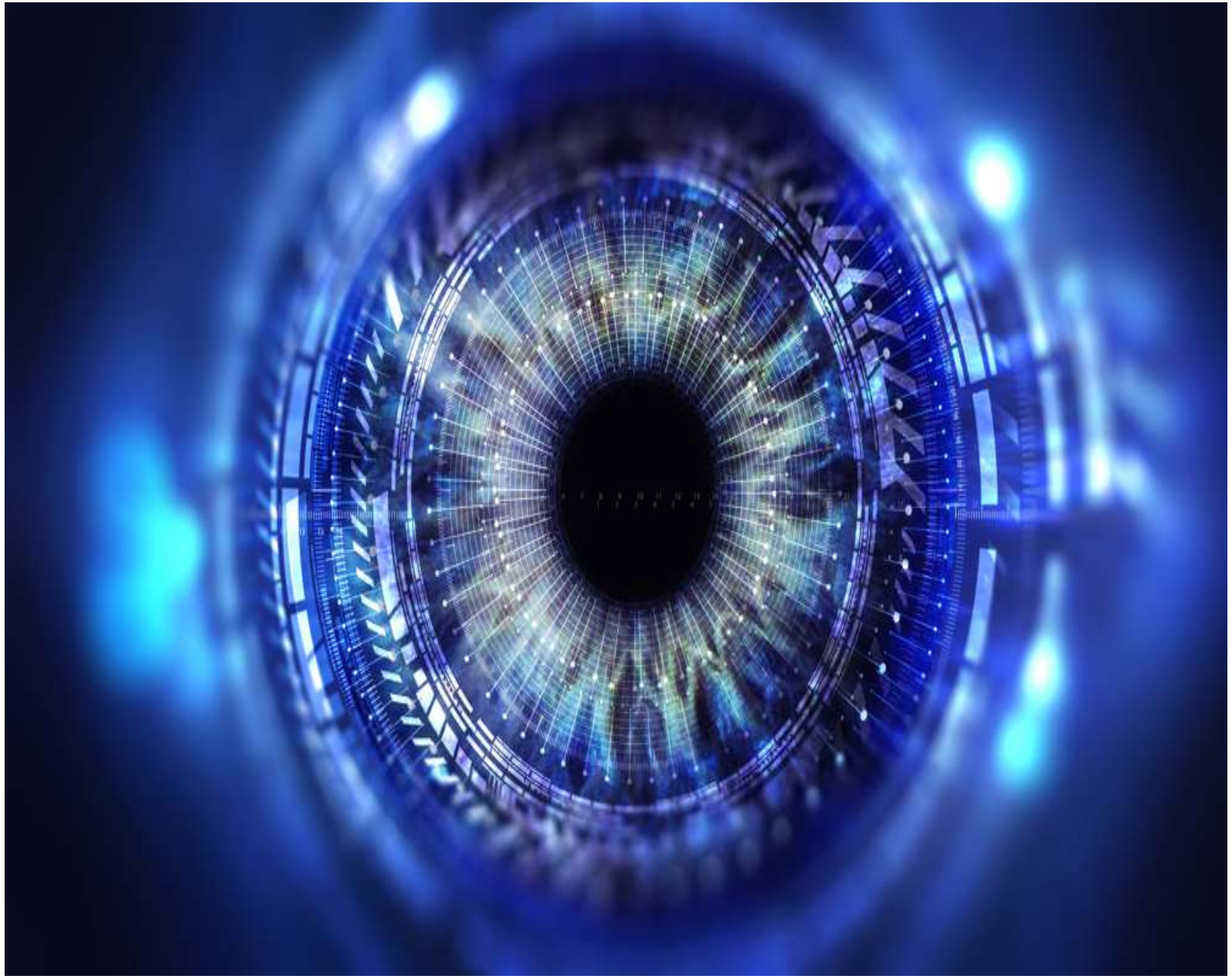
Symantec Blog publie des recherches détaillées sur des malwares bancaires et des techniques utilisées par SpyEye

URL : https://www.broadcom.com/blog

Sites Web de sécurité et plateformes de renseignement sur les menaces :VirusTotal Une plateforme qui analyse des fichiers malveillants et des URL suspectes. Elle permet de vérifier si un fichier ou un domaine est associé à des menaces comme SpyEye URL : https://www.virustotal.com/ , Botnet Tracking par Abuse.ch est une plateforme de renseignement sur les menaces qui suit les botnets, y compris ceux utilisés par SpyEye. URL : https://www.abuse.ch/

RÉSUMÉ DES POINTS TECHNIQUES DE SPYEYE

- **Injection HTML** pour tromper l'utilisateur et collecter des informations supplémentaires.
- **Keylogging** pour capturer les saisies de l'utilisateur.
- **Man-in-the-Browser** pour manipuler les transactions bancaires en temps réel.
- **Évasion des antivirus et anti-sandboxing** pour éviter la détection.
- **Serveur C&C** pour la communication avec les attaquants et la mise à jour des commandes.



MERCI POUR VOTRE ATTESTION