

SYNACKTIV

DIGITAL SECURITY

Penetration Tests

Red Team

Training

R&D

Reversing

Security audits **Code review**

Vulnerability research

Exploits



HOUDINI

Système embarqué pour la
réalisation de tests d'intrusion





HOUDINI

Systeme embarqué pour la réalisation de tests d'intrusion



OBJECTIFS

- Mettre en place un canal sécurisé entre un réseau interne et un serveur externe de type C&C
- Réduire le temps des intrusions physiques
- Faciliter la phase d'intrusion en profondeur lors d'une prestation de type Red Team
- Maximiser la probabilité d'établissement du canal sécurisé par la mise en œuvre automatisée de techniques d'évasion adaptatives
- Permettre la réalisation de tests d'intrusion internes à distance afin de réduire les coûts liés aux détachements des experts sur site

INNOVATIONS

- Miniaturisation • Automatisation • Flexibilité • Discrétion

FONCTIONNALITÉS

- **Systeme générique facilement dissimulable**
 - Miniaturisation de la plateforme
 - Discrétion du dispositif physique par l'insertion de la plateforme dans un objet de tous les jours
 - Indépendance de la plateforme vis-à-vis de l'objet englobant
 - Discrétion logique par la réduction de l'empreinte numérique du dispositif
- **Automatisation de la méthodologie d'évasion**
 - Analyse passive ou active de l'environnement réseau et récupération d'informations
 - Mise en oeuvre d'un algorithme d'évasion adaptatif afin de découvrir le canal de sortie le plus fiable
 - Protocole de sortie adapté aux problématiques réseaux (faible débit, interruption de service)
- **Adaptabilité à l'environnement**
 - Support des technologies réseaux Ethernet, Wi-Fi et 3G/4G
 - Contournement des systèmes d'authentification réseau du type 802.1x
 - Canal de sortie multi-protocoles (TCP, SSL, HTTP, DNS)

EXPERIENCE
CLIENT

SANS HOUDINI, couplage fort entre intrusion physique et logique lors des tests Red Team : intrusion physique, connexion au réseau interne, tests manuels, évacuation. Augmentation significative des risques de détection.

AVEC HOUDINI, faible couplage : intrusion physique, dépôt du dispositif et évacuation. Durée des intrusions physiques drastiquement réduite.

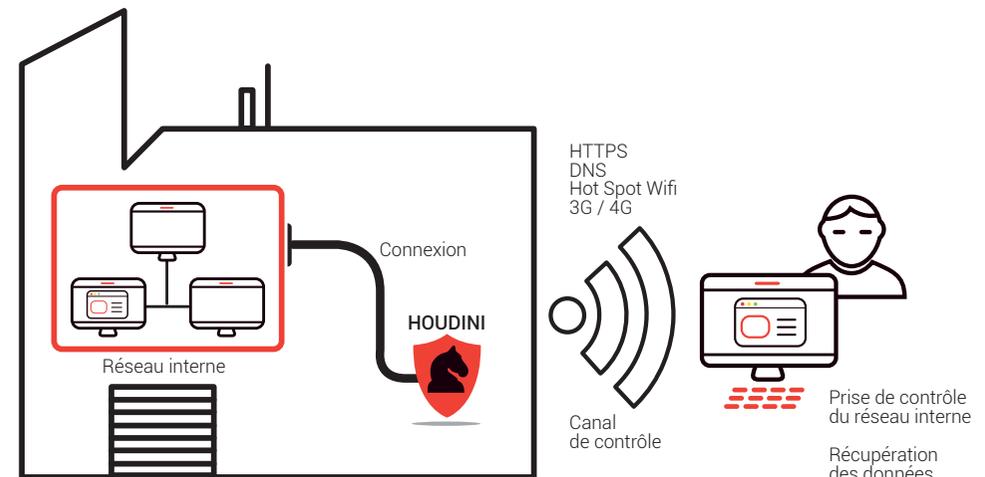


Gestion d'une flotte de systèmes Houdini

- Serveur C&C unique pour la gestion de plusieurs instances Houdini
- Prise de contrôle à distance des systèmes
- Mécanisme de blacklisting d'instances

Sécurité de la couche transport

- Flux d'administration du système et d'accès au réseau interne sécurisés au moyen de SSH



DÉCOUVREZ
NOS AUTRES
PRODUITS



KRAQZORUS
Plateforme centralisée de passage
d'empreintes de mots de passe



DISCONET
Automate collaboratif pour la
réalisation de tests d'intrusion



OURSIN
Plateforme d'attaques
par spear phishing



- **Synacktiv** est une société d'expertise en sécurité des systèmes d'information fondée en 2012 par des consultants ayant plus de 10 ans d'expérience dans le conseil et l'audit de systèmes informatiques.
- **Synacktiv** dispose du savoir-faire et des derniers outils et méthodologies pour aider ses clients à évaluer et améliorer le niveau de sécurité de leur système d'information.
- **Synacktiv** intervient en France et dans le monde entier.
- **Synacktiv** est un Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI) agréé par l'ANSSI.
- **Synacktiv** est un organisme certificateur autorisé par l'ARJEL (Autorité de Régulation des Jeux En Ligne).

Domaines d'intervention

Sécurité des systèmes d'information

Tests d'intrusion et audits de sécurité

Tests d'intrusion
Intrusions Red Team
Outils offensifs

Audits de code
Audits d'architecture
Recherche de vulnérabilités

ARJEL
CESTI CSPN

Systèmes d'exploitation ■ Terminaux mobiles ■ Applications web et cloud
Systèmes embarqués ■ Progiciels de gestions

Assistance sécurité

Développement ■ Conseil ■ Formations

Principes Fondateurs

Expertise



Nous recrutons et permettons aux meilleurs experts techniques de continuer à développer leur savoir-faire en sécurité informatique. Nous sommes capables de répondre aux besoins des clients les plus exigeants.

Pertinence



Nous travaillons à répondre précisément aux demandes de nos clients et à mettre l'accent sur les points qu'ils jugent importants. Nos méthodologies s'adaptent aux besoins spécifiques de chaque client.

Innovation



Nous améliorons constamment nos méthodologies et nos outils pour être plus pertinents et plus efficaces dans notre approche. Nous trouvons des solutions innovantes aux problèmes uniques de nos clients.

Transparence



Nous sommes transparents sur nos compétences et nos propres limites. Nous n'hésitons pas à orienter nos clients vers un autre prestataire si nous ne sommes pas les plus à même de traiter une demande.

**SYNACKTIV**
DIGITAL SECURITY

