THEIA SECURITY DATA NETWORK VOTRE

PARTENAIRE CYBERSECURITE

THEIA
SECURITY DATA NETWORK

WWW.THEIA-SDN.COM

Nos solutions de cybersécurités avancées

Découvrez notre gamme complète de solutions conçues pour protéger efficacement vos entreprises et collectivités

GUARDIA
BY THEIA-SDN

YAMI
BY THEIA-SDN

SPARTA
BY THEIA-SDN

ATTAQUE

SOC/SIEM souverain

Notre SOC, basé en France, assure une protection complète avec EDR et SIEM, une réponse rapide aux incidents, une détection en temps réel du chiffrement, plus de 3000 règles personnalisées pour une détection fine, une analyse des vulnérabilités et une conservation des données sur six mois.

SURVEILLANCE

Fuite de données sur le darknet

Notre système offre des alertes immédiates en cas de détection de fuites, identifie les données exposées pour des contre-mesures rapides, anticipe les cyberattaques par l'analyse des forums, et assure un accompagnement des services enquêteurs

www.theia-sdn.com

DEFENSE

Audits et tests d'intrusions

Notre service allie souveraineté technique et humaine, avec une expertise éprouvée et des certifications reconnues. Nous proposons un outillage packagé en interne et un entraînement régulier aux techniques de contournement. Les auditeurs ont accès à notre SOC/SIEM GUARDIA pour enrichir les analyses d'attaques

THEIA
SECURITY DATA NETWORK

YAMI

BY THEIA-SDN

Notre outil d’alerte d’exfiltration de données sur le darknet, dédié aux entreprises et collectivités

THEIA

SECURITY DATA NETWORK

AMI, notre outil d'alerte d'exfiltration de données sur le darknet, dédié aux entreprises et collectivités

Bases de données	Comptes compromis	InfoStealer	Identifiants compromis
927	14 447 469 301	44 533	10 600 849

- Être alerté dès la détection d'une fuite de données
- Identifier les données déjà exposées pour prendre les contre-mesures
- Anticiper une future cyberattaque par l'analyse des forums de discussion
- Prévenir des actions d'activistes violents (personnes physiques ou biens)
- Accompagner les services enquêteurs

THEIA
SECURITY DATA NETWORK

YAMI : les informations disponibles

Est-ce que les identifiants de vos employés ont été exfiltrés ?
Login et mots de passe de vos employés exfiltrés via infoStealer ou site forum
Adresse mail – Nom – Prénom – Date – fuite de base de données/infoStealer – Téléphone - Adresse

Est-ce que des infoStealers ont infecté votre organisation ?
Données collectées et exfiltrées depuis des machines infectées
InfoStealer (Nom du malware) – computerName – date - IP – fichiers exfiltrés

Quelle est la dernière fois que vos données sensibles ont été exposées ?
Date de la dernière exposition ou exfiltration des données
Date – infoStealer/fuite de base de données – ID Channel Telegram

Est-ce que quelqu'un a mis en vente vos données sur le blackmarket ?
Données en vente sur les forums
Nom BlackMarket - ID Channel Telegram - Date

Est-ce que l'on parle de vous sur le darkweb, et qui ?
Mentions de votre entreprise sur des channels Télégram, sites pirates ou blackmarket
ID Channel Telegram, nom du blackmarket, nom du site

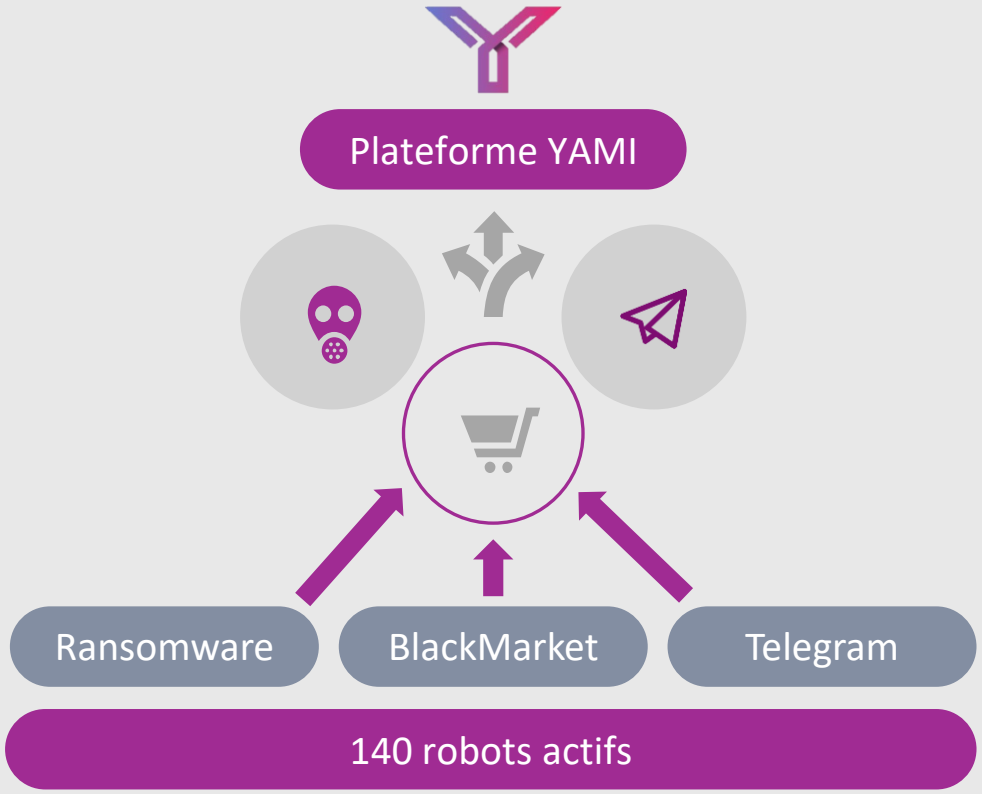
THEIA
SECURITY DATA NETWORK

YAMI : les sources de données

Groupes de Ransomware
Surveillance de 408 groupes
Parmi 1573 sites, dont 78 en ligne

BlackMarkets
204 market forum surveillés
Parmi 117 différents, dont 50 en ligne

Telegram
284 channels Telegram surveillés en continu



THEIA
SECURITY DATA NETWORK

YAMI : plus qu’un outil, une solution de surveillance complète

Une solution de surveillance avec **un accès complet à nos bases** pour chaque nom de domaine

Accès à notre support dédié pour vous accompagner dans **l’analyse des données collectées**

Notre solution comprend :

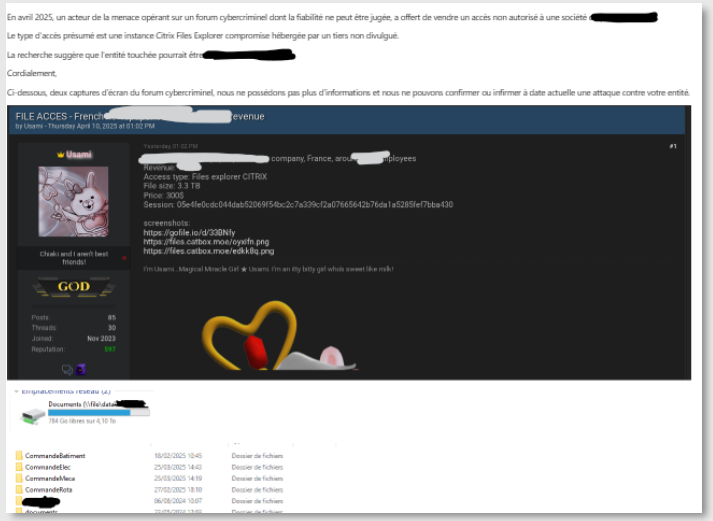
- Souscription annuelle par nom de domaine surveillé
- Accès au support (2 demandes par mois maximum)
  - Ex. Recherche par mot clé opérée par nos équipes dans le respect du RGPD
- Rapport d’analyse de recherche

THEIA
SECURITY DATA NETWORK

Cas d'usage de nos services et notre outil YAMI

10h00 – Alerte du CERT-FR

Un cybercriminal revendique posséder login/mdp d'un accès VPN d'un administrateur.
Il propose un accès à 3,5To de données sensibles. Les accès sont vendus 300$

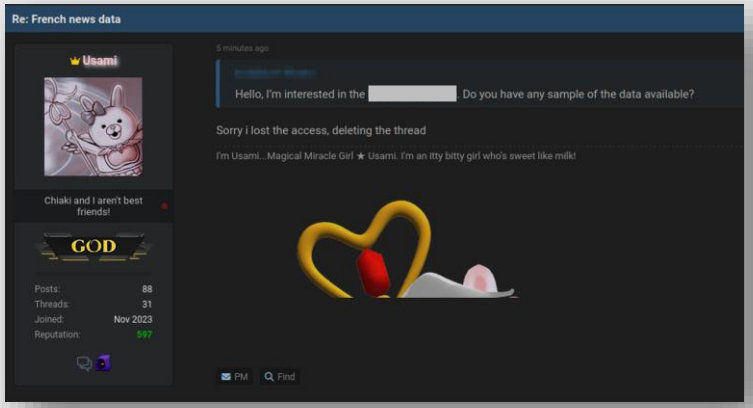


10h15 – Changement des mots de passe

L'organisation attaquée fait changer préventivement tous les mots de passe

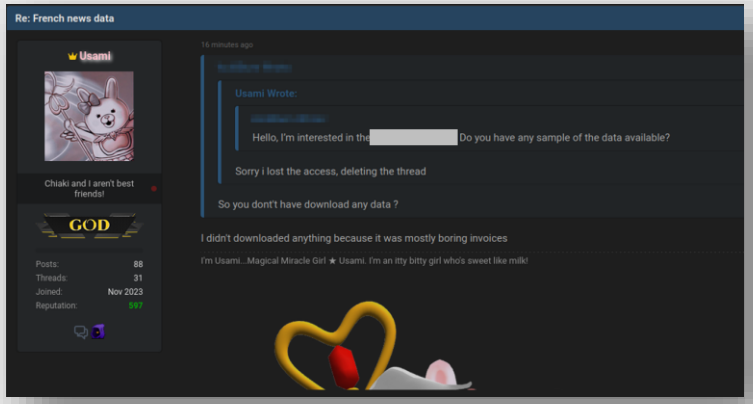
10h30 – Echanges avec le cyber criminel sur le forum

Le cybercriminel confirme avoir perdu l'accès au VPN



10h41 – Echanges

Le cybercriminel nous informe ne pas avoir pris le temps d'exfiltrer des données



11h43 – Suppression du post du cybercriminel

Comme le cybercriminel n'a plus rien à vendre, et que nous considérons ses propos fiables au regard de sa réputation, le post sur le forum est supprimé par un administrateur

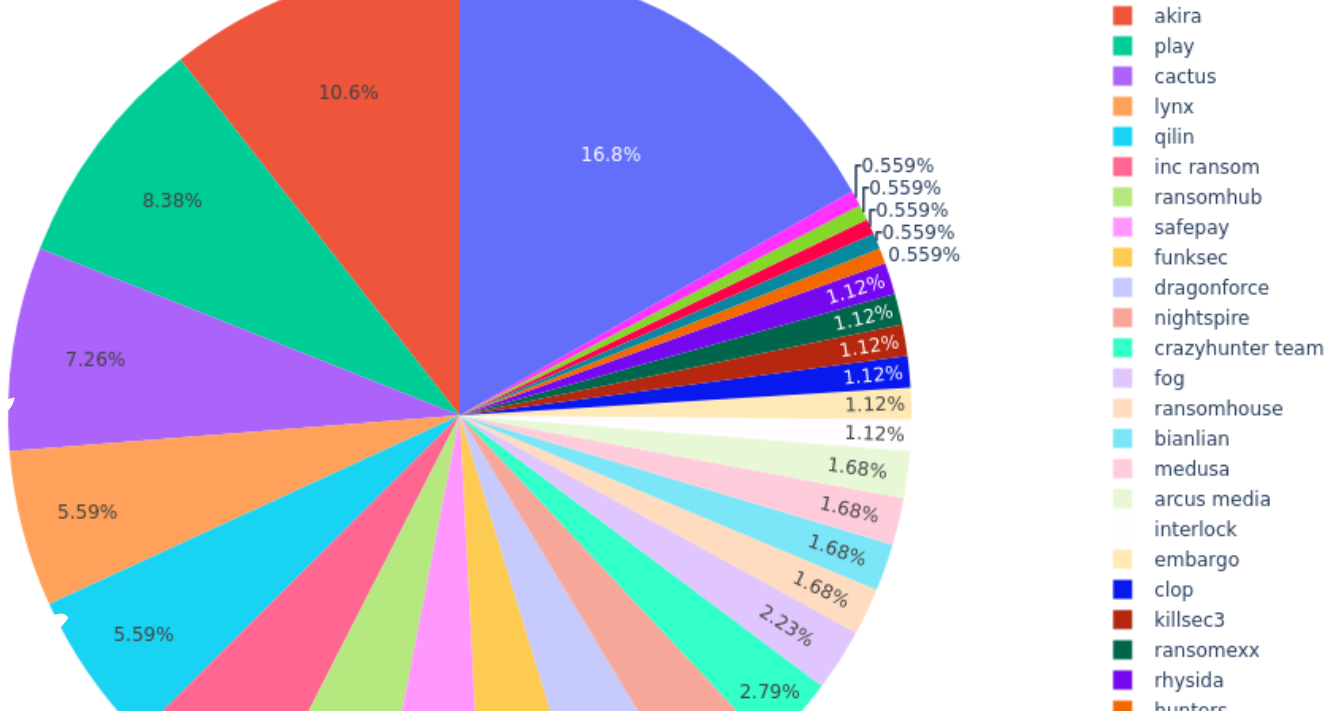
J + 48H – Rapport détaillé

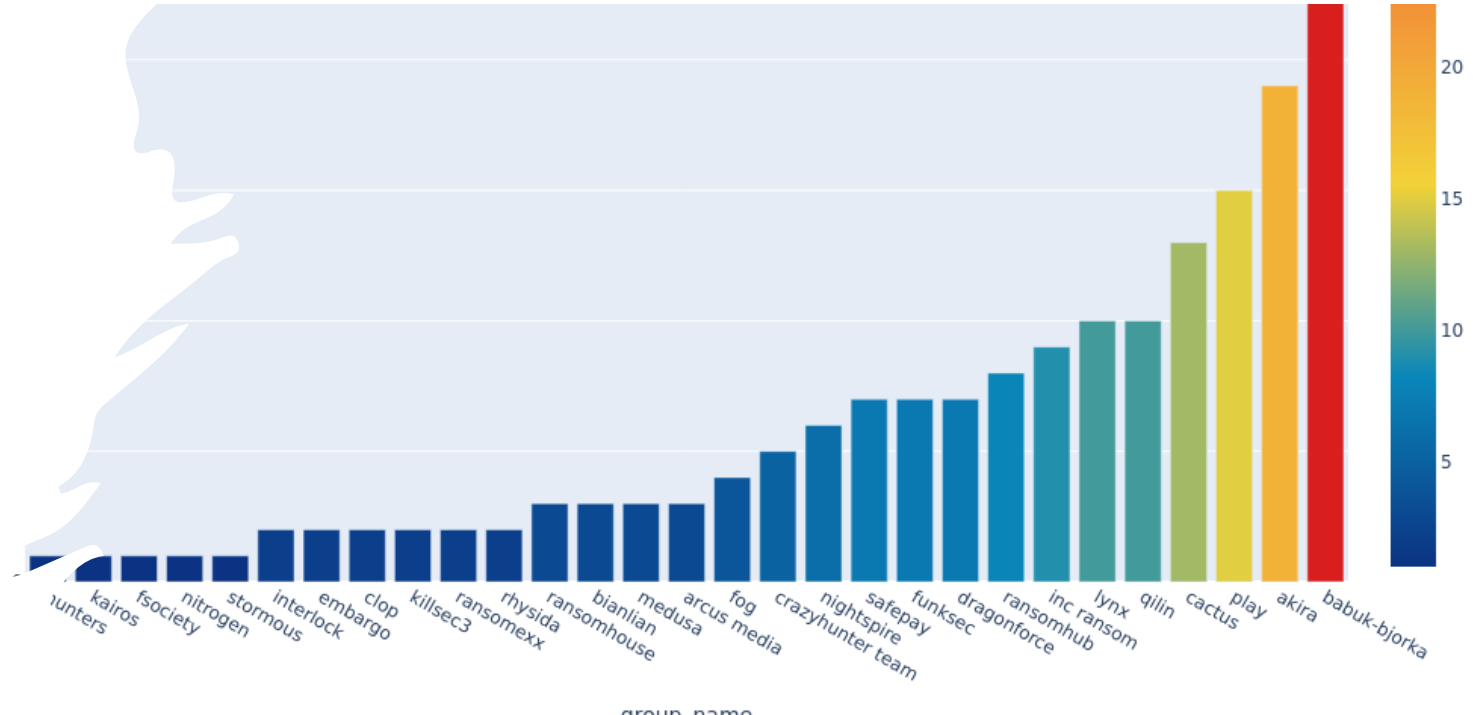
L'outil YAMI nous permet d'identifier à posteriori la source du piratage par infostealer, tels le nom, prénom, adresse IP du poste. Nous restituons la chronologie des évènements

THEIA
SECURITY DATA NETWORK

YAMI
vision consolidée des informations liées à votre entreprise ou collectivité

Exemple
Activité des groupes de ransomware sur 7 jours
Nombre de revendications d'attaques
Du 07 au 13 mars 2025





THEIA
SECURITY DATA NETWORK

THEIA SECURITY DATA NETWORK VOTRE

PARTENAIRE CYBERSECURITE

THEIA
SECURITY DATA NETWORK

WWW.THEIA-SDN.COM