

SECURE DNS

FILTRAGE DNS, HÉBERGÉ EN SUISSE

BLOQUÉ, DGA

Requête malveillante vers q7vk2x0pzt4rl.top

Depuis 10.20.40.17 sur le réseau
des serveurs, 08:14:03. Deux autres
noms générés ont suivi en moins de
50 ms.

TOUT COMMENCE PAR UNE REQUÊTE DNS.

En une journée de travail ordinaire, le navigateur d'un seul utilisateur contacte des centaines de domaines que personne n'a choisi de visiter : régies publicitaires, traceurs, contenus intégrés à d'autres pages. Certains hébergent du phishing, des arnaques ou des logiciels malveillants, et changent de nom assez souvent pour échapper à la plupart des listes de blocage.

Bien des appareils du réseau n'ont même pas d'utilisateur. Imprimantes, caméras et automates OT interrogent le DNS jour et nuit, sans que personne ne regarde ce qu'ils demandent.

Secure DNS répond à ces requêtes depuis des résolveurs qu'EXYS exploite en Suisse. Chaque nom est comparé à une base de domaines malveillants qu'EXYS reconstruit chaque jour à partir de sources externes et de ses propres données. Un domaine malveillant ne reçoit aucune réponse : la page ne se charge pas et le logiciel malveillant n'atteint pas son serveur.

Pour passer à Secure DNS, il suffit de modifier un réglage DNS de votre réseau. Rien à installer, et chaque appareil qui interroge le DNS est protégé immédiatement.

**LES DOMAINES MALVEILLANTS CHANGENT DE NOM CHAQUE JOUR.
NOTRE BASE DE DONNÉES AUSSI.**

DES NOMS QUI N'EXISTAIENT PAS HIER

Certains logiciels malveillants n'ont pas d'adresse fixe pour leur serveur de commande et de contrôle. Ils génèrent chaque jour de nombreux noms d'apparence aléatoire et les essaient jusqu'à ce que l'un d'eux réponde. Aucune liste ne peut suivre ce rythme. Secure DNS analyse donc aussi le nom lui-même : le traitement automatique du langage distingue un nom généré d'un vrai nom, même s'il n'a jamais été vu.

CE QUE VOUS VOYEZ

Vous recevez chaque jour un rapport par e-mail, également disponible dans le portail. Il indique ce qui a été bloqué, par site et par plage d'adresses IP. Sur demande, EXYS adapte vos listes d'autorisation et de blocage.

CE QUI EST INCLUS :

- Résolveurs hébergés et exploités par EXYS en Suisse
- Chaque appareil qui interroge le DNS est couvert, y compris les équipements IT et OT sans surveillance
- Blocage des domaines de phishing, d'arnaque, de logiciels malveillants et de jeux d'argent
- Apprentissage automatique sur le nom de domaine pour repérer les domaines générés par algorithme, même inédits
- Rapport quotidien par e-mail et dans le portail, par site et par plage d'adresses IP
- Plus de 2,5 millions de requêtes DNS traitées par mois
- Un seul réglage DNS à modifier sur votre réseau, rien à installer
- Base de domaines malveillants reconstruite chaque jour à partir de sources externes et des données d'EXYS
- Aucune réponse à une requête bloquée : le logiciel malveillant n'atteint pas son serveur de commande
- Vérification supplémentaire dans la base EXYS d'adresses IP et d'URL malveillantes
- Analyse détaillée en option, avec indicateurs de risque et recommandations

RESOLVER 1. QUERY STREAM				TYPE	D
TIME	CLIENT	QUERY			
08:14:02.118	10.20.12.31	login.microsoftonline.com		A	1
08:14:02.164	10.20.12.31	outlook.office365.com		AAAA	1
08:14:02.390	10.20.14.7	cdn.jsdelivr.net		A	1
08:14:02.411	10.20.14.7	office365-mailbox-quota.site		A	1
08:14:02.733	10.20.12.58	www.admin.ch		A	
08:14:03.002	10.20.40.17	q7vk2x0pzt4r1.top		A	
08:14:03.019	10.20.40.17	h3m9wq1ckz8o.xyz		A	
08:14:03.044	10.20.40.17	z0rt6pl2vbn5yq.biz		A	
08:14:03.250	10.20.12.31	teams.microsoft.com		AAAA	
08:14:03.512	10.20.15.92	fonts.gstatic.com		A	
08:14:03.640	10.20.15.92	parcel-redelivery-ch.info		A	
08:14:03.871	10.20.21.4	time.windows.com		A	
08:14:04.106	10.20.12.58	www.sbb.ch		A	
08:14:04.322	10.20.30.12	update.googleapis.com		A	
08:14:04.380	10.20.30.12	invoice-docs-share.online		A	
08:14:04.517	10.20.14.7	api.github.com		A	
08:14:04.776	10.20.40.17	w4y8nq0t2jx6.click		A	
08:14:05.041	10.20.12.31	slack.com		A	
08:14:05.268	10.20.21.4	ocsp.digicert.com		A	
08:14:05.390	10.20.15.92	www.linkedin.com		A	
08:14:05.611	10.20.12.58	secure-ebanking-ch-login.top		A	

CONTACTEZ-NOUS

ADRESSE

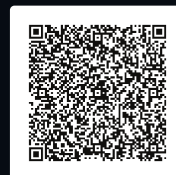
EXYS SA
Strada Regina 16
CH-6934 Bioggio
Tessin, Suisse

CONTACT

Tél. +41 (0)91 220 52 00

www.exys.swiss
office@exys.swiss

EXYS SA est certifiée ISO/IEC 27001



EXYS
WHERE PASSION
MEETS TECHNOLOGY

EXYS5100 - SECURE - DNS