

SECURE DNS

FILTRO DNS OSPITATO IN SVIZZERA

OGNI CONNESSIONE INIZIA DAL DNS.

In una normale giornata di lavoro, il browser di un solo utente contatta centinaia di domini che nessuno ha scelto di visitare: reti pubblicitarie, tracker, contenuti incorporati in altre pagine. Alcuni ospitano pagine di phishing, truffe o malware e cambiano nome così spesso da sfuggire alla maggior parte delle liste di blocco.

Buona parte della rete non ha nemmeno un utente. Stampanti, telecamere e controllori OT inviano richieste DNS giorno e notte e nessuno controlla quali domini cercano.

Con Secure DNS, queste richieste passano dai resolver che EXYS gestisce in Svizzera. Ogni dominio viene confrontato con un database di domini malevoli che EXYS aggiorna ogni giorno da fonti esterne e proprie. Le richieste verso un dominio malevolo non ricevono risposta: la pagina non si carica e il malware non raggiunge il suo server C2.

Per attivarlo basta cambiare i server DNS della rete. Nessun agente da installare: da quel momento è protetto ogni dispositivo che invia richieste DNS.

BLOCCATO, DGA

**Richiesta malevola a
q7vk2x0pzt4rl.top**

Da 10.20.40.17 (rete server),
08:14:03. Entro 50 ms, altre due
richieste verso domini generati.

**OGNI GIORNO NASCONO NUOVI DOMINI MALEVOLI.
IL NOSTRO DATABASE SI AGGIORNA OGNI GIORNO.**

DOMINI GENERATI DA ALGORITMI

Alcuni malware non hanno un indirizzo fisso per il server di comando e controllo (C2): generano ogni giorno molti nomi casuali e li provano finché uno risponde. Nessuna lista di blocco riesce a stare al passo. Secure DNS analizza anche il nome di dominio: un modello di elaborazione del linguaggio naturale distingue un dominio generato da un algoritmo (DGA) da uno legittimo, anche se non è mai stato visto prima.

VISIBILITÀ

Ogni giorno arriva via email un report, disponibile anche nel portale. Mostra cosa è stato bloccato, per sede e per sottorete. Su richiesta, EXYS aggiorna gli elenchi dei domini bloccati e consentiti.

COSA È INCLUSO:

- Resolver ospitati e gestiti da EXYS in Svizzera
- Protetto ogni dispositivo che invia richieste DNS, compresi i dispositivi IT e OT non presidiati
- Bloccati i domini di phishing, truffe, distribuzione di malware e gioco d'azzardo
- Apprendimento automatico sul nome di dominio per riconoscere i domini DGA, anche se mai visti prima
- Report giornaliero via email e nel portale, per sede e sottorete
- Oltre 2,5 milioni di richieste DNS gestite al mese
- Basta cambiare i server DNS della rete: nessun agente da installare
- Database dei domini malevoli aggiornato ogni giorno da fonti esterne e dalla threat intelligence di EXYS
- Le richieste bloccate non ricevono risposta, così il malware non raggiunge il server C2
- Richieste verificate anche nel database di threat intelligence EXYS con IP e URL malevoli
- Analisi dettagliata opzionale con indicatori di rischio e raccomandazioni

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	

CONTATTI

INDIRIZZO

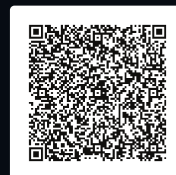
EXYS SA
Strada Regina 16
CH-6934 Bioggio
Ticino, Svizzera

CONTATTO

Telefono +41 91 220 52 00

www.exys.swiss
office@exys.swiss

EXYS SA è certificata ISO/IEC 27001



EXYS
WHERE PASSION
MEETS TECHNOLOGY

EXYS5100 - SECURE - DNS