THREAT SHIELD BY YOROI

IL CYBER SCUDO A PROTEZIONE DELLA TUA AZIENDA

nethesis

nethesis

COMPUTERS & SOFTWARE
INNOVATIVE SOLUTIONS

Se arriva una mail di phishing in russo capisci subito che può essere una mail sospetta.

Ma **è facile cadere nel tranello se la mail è ben fatta**, in italiano corretto, con un mittente riconoscibile e con cui abbiamo a che fare quotidianamente.

Anche l'utente più accorto non riuscirebbe a trattenersi dal cliccare sul link riportato al suo interno.

Come evitare del tutto che ciò accada?

In Nethesis abbiamo cercato di risolvere il problema all'origine, bloccando tutti gli IP e siti sospetti indipendentemente dal protocollo utilizzato.

Abbiamo sviluppato una sorta di scudo a protezione della tua azienda: **il Threat shield.**

Questo nuovo servizio blocca i siti sospetti indipendentemente da come l'utente cerchi di accedervi: navigando su internet, eseguendo download a siti web ritenuti malevoli o cliccando su link contenuti nelle email.

Come funziona questo cyber scudo?

Analizza tutte le minacce presenti nel mercato mondiale, le cataloga e blocca all'istante, interrompendo istantaneamente tutto il traffico da/verso gli host internet malevoli o compromessi.

I cataloghi vengono continuamente aggiornati grazie al servizio sviluppato in partnership con Yoroi, azienda italiana esperta in cyber security.

Sfruttando le potenzialità dell'intelligenza Artificiale, Yoroi raccoglie e **integra le informazioni sugli IP e nomi malevoli,** ottenute dai principali sistemi globali di analisi delle infezioni e attacchi informatici.

Perchè è così potente?

L’efficacia di questo servizio è direttamente legata alla qualità delle informazioni fornite da Yoroi, tipicamente disponibili solo in ambiti Enterprise e ora utilizzabili anche da partner e clienti Nethesis.

Il servizio di Yoroi è caratterizzato da:

- **Elevata qualità delle liste** ricavate da fonti eterogenee e soggette a continue analisi di specialisti
- **Efficacia massima su campagne malware** indirizzate verso la zona geografica Italia/Europa
- **Livello di confidenza** molto elevato, quindi bassissima percentuale di falsi positivi

Blocchi basati anche su DNS

IL DNS è sempre più spesso usato dai malware per connettersi ai server *Command and Control*, in tal senso diventa una risorsa molto importante e può essere usata per bloccare queste connessioni illecite.

Tramite le blacklist DNS, integrate nello Threat Shield, è possibile aggiungere un altro strato di protezione **bloccando le richieste fatte a domini malevoli.**

In pratica tutte le richieste DNS fatte dai client (PC, device mobili e server) vengono inoltrate in modo trasparente ad un proxy DNS presente sul firewall aziendale NethSecurity. I domini presenti in blacklist non vengono risolti con il relativo IP bloccandone di fatto la connessione.