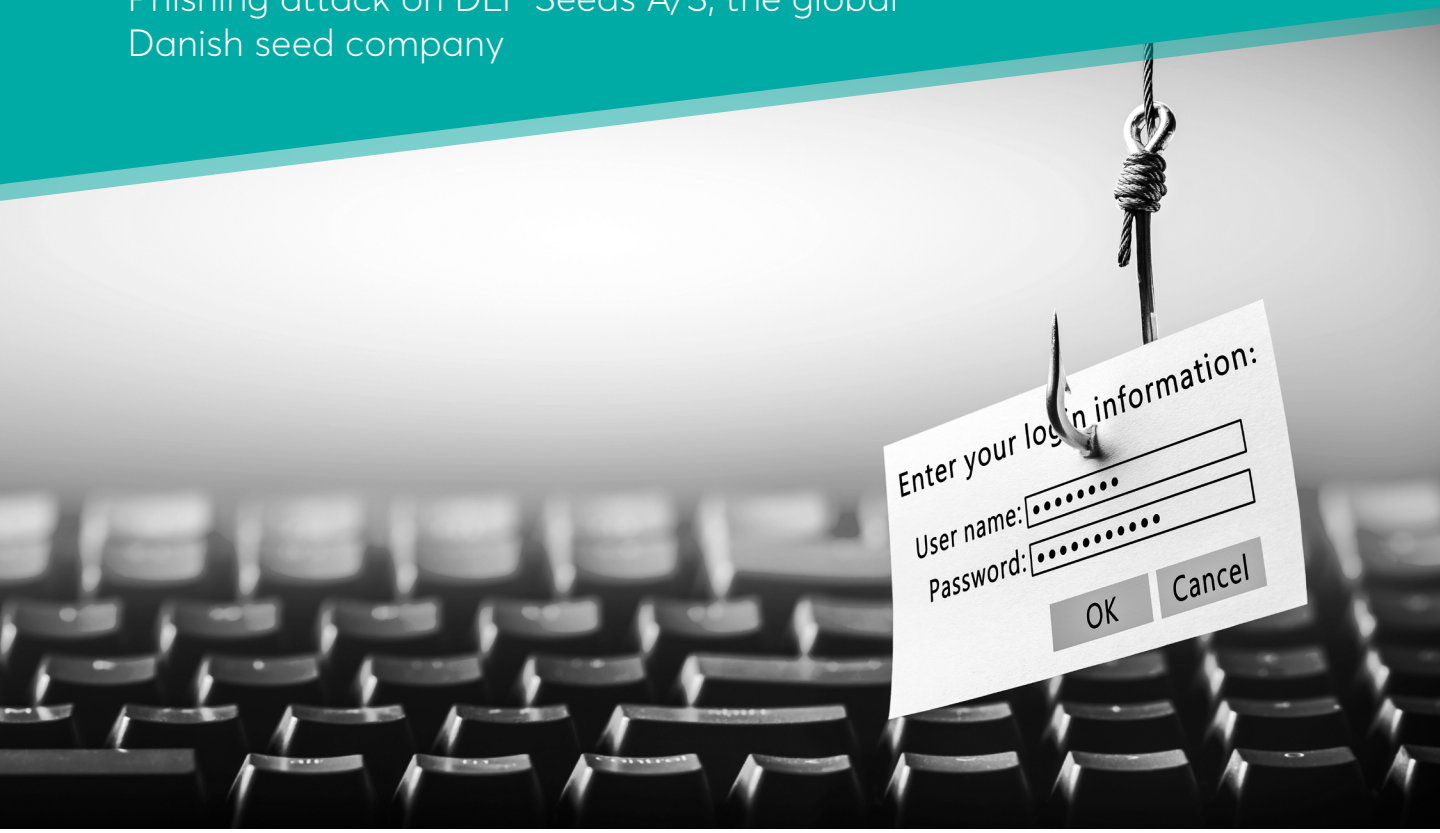
CSIS
REST ASSURED

JANUARY 11, 2023

MANAGED DETECTION & RESPONSE

Incident case

Phishing attack on DLF Seeds A/S, the global Danish seed company



THE POWER OF OUR MDR SERVICE

CSIS detected and fully resolved the phishing attack incident in less than an hour.

THE ATTACKER'S INTENTION

The main objective of the perpetrators was to compromise at least one user's credentials to enable lateral movement and escalation. To make this happen, they used a sophisticated spear-phishing approach to target several specific users.

The criminals implemented this targeted attack with the usernames of the targets encoded and embedded in the link they received via email and used an email subject line that matched regular team notifications. Moreover, the layout of the phishing site mimicked the company's legitimate website completely, making it significantly more challenging to detect the deceit.

CSIS IN ACTION

Based on our constantly evolving detection rules and leveraging Microsoft Defender for Endpoint (MDE), we detected the phishing attack and notified the customer immediately through our Threat Intelligent Platform and a Critical Incident Call.

Using MDE's sandboxing function and a decoding technique, our team succeeded in spotting all links embedded in the phishing emails and preemptively blocked them.

Continued on next page…

Continued from previous page...

Having assessed the full scale of the attack, we identified the users that had already clicked on the infected link. We proceeded to confirm the integrity of each mailbox, searching for forwarding rules and other malicious attempts at facilitating exfiltration.

All required actions were taken quickly, including blocking the sender, deleting emails, resetting user credentials, and revoking all sessions.

OUR HIGHLIGHTS

Phishing attacks continue to be prevalent and are still one of the most effective means for cybercriminals to compromise an organization. Spear-phishing attacks can be extremely well-designed and sophisticated and, the biggest challenge is that an attacker only needs one entry point to initiate an incident.

Rapid detection and follow-up actions are a must. Phishing attacks can become full-blown incidents involving serious damage to an organization, including exfiltrated and leaked data.

However, getting a full and correct understanding of an attack cannot become a trade-off to ensure a fast response. It is essential to correctly understand the scale and scope to ensure that remediation actions are comprehensive and effective.