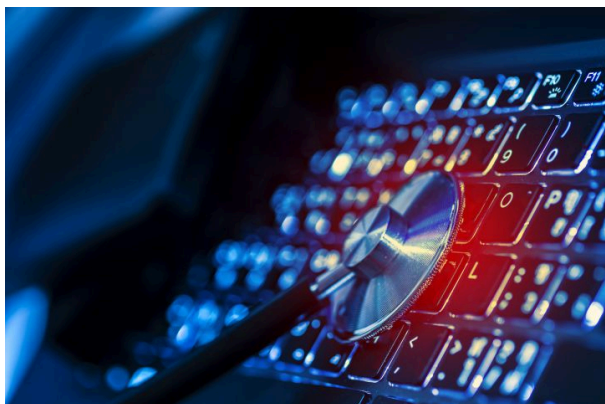


# Defray Ransomware Sets Sights on Healthcare and Other Industries - Wiadomości bezpieczeństwa

Archived: 2026-04-05 16:47:46 UTC



Widespread [ransomware](#) attacks are becoming more common, but while the usual “spray and pray” methods allow ransomware to affect the most number of victims possible, other strategies are more discriminatory.

The newly discovered Defray (detected by Trend Micro as [RANSOM\\_DEFRAY.A](#) and [RANSOM\\_DEFRAY.B](#)) ransomware employs a more targeted approach. [Reports](#) say that Defray distributors are pursuing healthcare, education, manufacturing, and technology organizations using a tailored [social engineering](#) strategy. These industries, [healthcare specifically](#), have always been particular favorites of ransomware authors.

## Defray behavior and demands

As with most ransomware, Defray is spread through phishing emails which try and coerce victims into downloading a malicious file. The proliferation of ransomware through email is well-documented. A [2016 report by Trend Micro](#) found that email was the most common entry point, with 79% of ransomware detected coming from spam mail.

Luckily, the Defray attacks have been [relatively small](#), and so far only minor campaigns have been tracked. The phishing emails the authors use are well-crafted—for an attack targeting a hospital, the phishing email was from a “hospital IT manager” and the malicious files were disguised as patient reports. In other emails, the attackers masqueraded as a UK-based aquarium company asking for a quote or order, and the malicious file had an “official” logo attached. The specificity and detail show a definite effort to convince targets of their legitimacy, and the more tailored lures show the attackers are investing in more specific targets.



Deep Security™ provides protection via the following DPI rule:

- 1008572-Ransomware Defray

For TippingPoint the applicable rule is:

- 29521: HTTPS: Defray Ransomware Data Exfiltration

HIDE

**Like it? Add this infographic to your site:**

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

---

Source: <https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/defray-ransomware-sets-sights-on-healthcare-and-other-industries>