THIRDWATCH

CASE STUDY

BestSeller Ransomware Attack (2024-25)

Blackwired began tracking suspicious cyber activity against BestSeller, a Danish fashion company, in October 2024. Initial alerts flagged links to dark web domains associated with ransomware, signalling early-stage threat activity. By November 2024, threat intelligence confirmed a surge in malicious files and ransomware strains, prompting predictions of an imminent large-scale attack. Despite Blackwired's advanced warning, BestSeller chose to not pre-emptively implement the provided FastHunt DTI remediations. In November 2024, a ransomware attack exploiting the Fortijump vulnerability was confirmed by BestSeller. Blackwired responded by re-stating the DTI containment measures with added threat intelligence that would have limited the spread and removed the adversary's C2 control communications.

Blackwired used its "Aim, Ready, Fire" (ARFi) anticipatory risk model to predict this attack and provided actionable DTI to mitigate a major ransomware attack by a credible adversary.

1 AIM PHASE

EARLY THREAT DETECTION AT RECONNAISSANCE STAGE:

- On October 18, 2024, Blackwired detected early reconnaissance tied to the GandCrab dark web domain.
- This gave a three-week lead time for pre-incidence response (stop & contain).

2 READY PHASE

INFRASTRUCTURE SETUP

- By November 8, a surge in ThirdWatch's Direct Threat Intelligence (DTI) revealed 42 new executables and 202 ransomware variants, including Expiro, Moiva and Ryuk.
- Other malware malformations showed sustained increase from November to March.
- Consistent use of infrastructure—IP addresses, URLs and domains—aligning with malicious intent, was identified (including the download of a poisoned Fortinet operating system from an illegitimate website).

3 FIRE PHASE

ATTACK & RESPONSE

- On November 13, the "Fortijump exploit" was confirmed by BestSeller and a robotic wave attack confirmed Blackwired's prediction.
- ThirdWatch intelligence provided at the Aim / Ready stages could have enabled a swift pre-emptive containment response.

THIRDWATCH

CASE STUDY

BestSeller Ransomware Attack (2024-25)

Technical Edge

- Continuous zero-touch monitoring of direct threat risks.
- Identified the adversary's attacking infrastructure and actions as these evolved through the Aim Ready Fire (ARFi) stages, enabling clear threat visualization as it happens.
- Provision of ThirdWatch DTI countermeasures that, when operationalized, pre-emptively stops and contains the attack.

Why It Matters

Blackwired's foresight gave BestSeller crucial time to act, and the opportunity to prevent and/or reduce considerable damage. ThirdWatch intelligence enables organizations to visualize and understand direct threats to them and provides an actionable proactive mitigation solution that is not available through any other vendor.