SUCCESS STORY

flare

Manufacturing Company Manages External Risks After Ransomware Attack, Saving Up to 500 Hours Per Year

The Customer

The manufacturing company provides one-on-one, customized, quality engine repair & overhaul services for the Rolls-Royce Model 250 Series of engines & accessories

In operation for 35 years

For many companies, dark web monitoring remains a time-consuming manual process that requires a specialized skill set. Security analysts need to know how to access the dark web, hide in illicit forums, read foreign languages (and threat actor jargon), and study criminal groups' patterns.

Meanwhile, many threat intelligence feeds connect users to incomplete databases of leaked information, providing little context around the data. Without this context, security teams have no way to effectively use it, leaving it disconnected from the rest of their cybersecurity technology stack.

As attackers move from traditional dark web forums on Tor to newer technologies like illegal Telegram channels, the communications become even more decentralized. In response, organizations seek solutions that give them a single source of contextualized dark web monitoring data that integrates with their cybersecurity monitoring and ticketing tools.

> "After a ransomware attack, Flare was the last piece of the puzzle of boosting our cybersecurity approach. Instead of manually sourcing the dark web and other sources for hours, I can save up to 500 hours per year and have peace of mind with this Threat Exposure Management solution."
>
> **-President and General Manager, Manufacturing Company**

In addition, the number of ransomware attacks have skyrocketed in the last few years, with data extortion ransomware attacks increasing at an annualized rate of more than 112% in 2023. In our research, we observed that threat actors attacked the Manufacturing, Information Technology, and Professional Services industries the most in 2023.

To monitor illicit sources and stay vigilant for information stolen from a past attack, and to exercise ransomware readiness for the future, our customer implemented Flare into their cybersecurity program.

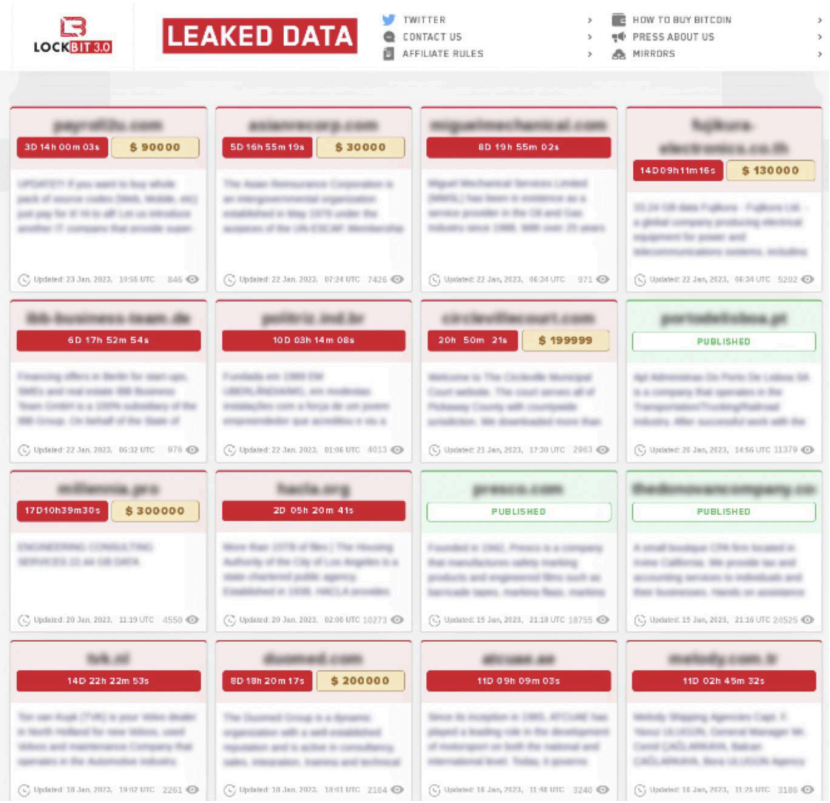
Challenge: Emotionally and Resource-Exhausting Manual Dark Web Monitoring After Ransomware Attack

Our customer knew that its security program needed to include dark web monitoring. The organization has a two-fold mission: protecting data and maintaining repair operations. Like many companies in aerospace and manufacturing verticals, their technology stack includes traditional IT and technologies with human-machine interfaces for their engine and machine shops.

Unfortunately, threat actors conducted a ransomware attack, which this manufacturing organization quickly contained, but there was the possibility the ransomware group extracted sensitive information. The President-General Manager spent hours manually scouring the dark web and other relevant sources looking for leaked files stolen in the attack as well as a part of ransomware readiness for any future risks. Additional concerns about manually searching the dark web are stumbling on malicious sites and awful content.

The manual process included looking into the following sources, sometimes until 3:00-5:00 AM in the morning:

- Ransomware websites
- Dark web chatter
- News events
- Educational resources from cyber practitioners across online communities and YouTube



Ransomware group Lockbit's website shares ransomware victims' stolen information

Implementation: Smooth Transition from Free Trial to Onboarding

The manufacturing company's President-General Manager ended up finding Flare, Threat Exposure Management (TEM) solution, through an educational video on dark web monitoring, and immediately signed up to access the free trial. He described the transition to using Flare and including it to the rest of their cybersecurity program as "very easy." In addition, the user interface is straightforward to navigate.

> "You're telling me what I was doing alone manually for hours, you can do it for me automatically?! Now instead of dealing with all my security machines I just look at one feed of my related content with Flare. I kick back and relax, not worry as much, and spend time on other pressing items."
>
> — President and General Manager, Manufacturing Company

Benefits: Up to 500 Hours Saved per Year

With Flare, our customer's security team:

- **Saves 5–10 hours of research per week** (and thus up to about 500 hours per year) by automating the research process
- Consolidates research into a **single feed of related events,** eliminating the need to manage various security machines
- Reduces stress related to feeling defenseless and overwhelmed
- Spends more time focused on other critical security tasks

With Flare's easy-to-use interface, our customer was able to rapidly transition from manual processes to automated monitoring, enabling a more efficient, informed, and proactive security program.