

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

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.

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.

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

“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

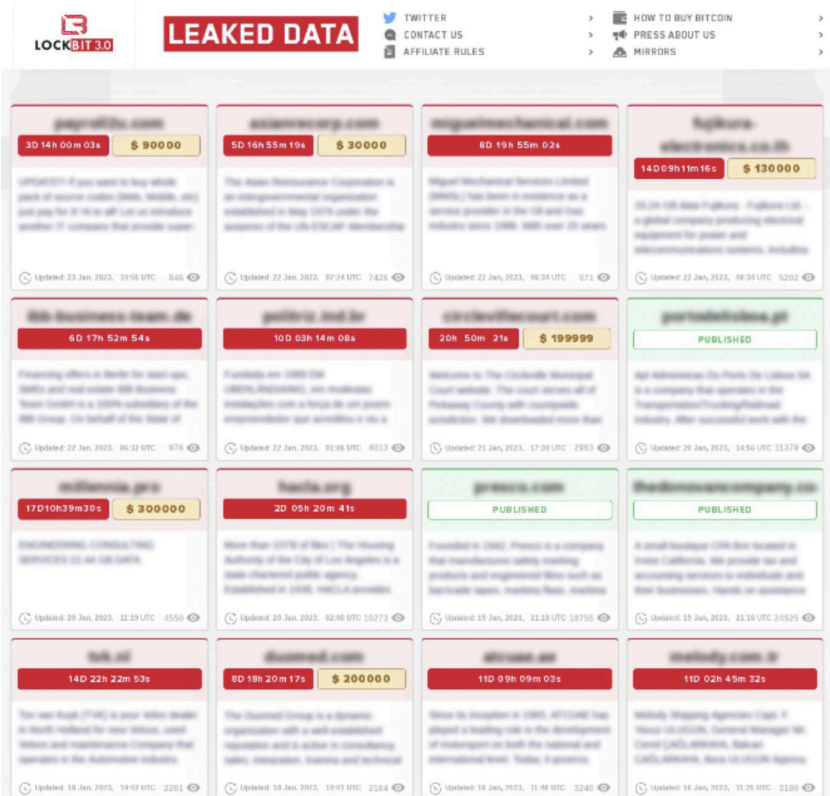
Challenge: Emotionally and Resource-Exhausting Manual Dark Web Monitoring After Ransomware Attack

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



The screenshot displays the Lockbit 3.0 ransomware website. At the top, there is a navigation bar with links for 'TWITTER', 'CONTACT US', 'AFFILIATE RULES', 'HOW TO BUY BITCOIN', 'PRESS ABOUT US', and 'MIRRORS'. Below the navigation bar, a prominent red banner reads 'LEAKED DATA'. The main content area is a grid of 16 listings, each representing a different data leak. Each listing includes a domain name, a timestamp, a price in Bitcoin, and a brief description of the leaked information. For example, the first listing is for 'www.offthecoast.com' with a price of \$90,000. The listings are arranged in a 4x4 grid.

Domain	Timestamp	Price	Description
www.offthecoast.com	3D 14h 00m 03s	\$ 90000	OFFSHORE If you want to buy whole pack of source codes (CMS, WP, etc) and pay for it in a 48h all can be made available if someone that provide want
www.offthecoast.com	5D 16h 55m 19s	\$ 30000	The Best Resource Corporation is an international organization established in May 2019 under the auspices of the UK's HM Revenue & Customs
www.offthecoast.com	6D 19h 55m 02s		Aligent Mechanical Services Limited (AMSL) has been in existence as a service provider in the UK and the industry since 1988. With over 25 years
www.offthecoast.com	14D 09h 11m 16s	\$ 130000	20.24 100 Data Platform - Platform Ltd - a global company producing electrical equipment for power and telecommunications systems, including
www.offthecoast.com	6D 17h 52m 54s		Financial offers in Berlin for next up, 100% and real estate 100 Business Team London is a 100% subsidiary of the 100 Group. On behalf of the State of
www.offthecoast.com	10D 03h 14m 08s		Founded in 1980, the 100 Group is a 100% subsidiary of the 100 Group. On behalf of the State of
www.offthecoast.com	20h 50m 21s	\$ 199999	Welcome to The Colorado Municipal Court website. The court serves all of Pitkin County with complete services. We distributed more than
www.offthecoast.com		PUBLISHED	Ag Administration On Paris On London UK is a company that operates in the Transportation/Travel/Hotel industry. After successful work with the
www.offthecoast.com	17D 10h 39m 35s	\$ 300000	International Criminal Police Organization (ICPC) has been in existence since 1975. It is a 100% subsidiary of the 100 Group. On behalf of the State of
www.offthecoast.com	2D 05h 20m 41s		More than 1000 of the 100 Group is a 100% subsidiary of the 100 Group. On behalf of the State of
www.offthecoast.com		PUBLISHED	Founded in 1980, the 100 Group is a 100% subsidiary of the 100 Group. On behalf of the State of
www.offthecoast.com		PUBLISHED	A small business (100 Group) has been in existence since 1975. It is a 100% subsidiary of the 100 Group. On behalf of the State of
www.offthecoast.com	14D 22h 22m 53s		The 100 Group (100 Group) is a 100% subsidiary of the 100 Group. On behalf of the State of
www.offthecoast.com	8D 18h 20m 17s	\$ 200000	The 100 Group is a 100% subsidiary of the 100 Group. On behalf of the State of
www.offthecoast.com	11D 09h 09m 03s		More than 1000 of the 100 Group is a 100% subsidiary of the 100 Group. On behalf of the State of
www.offthecoast.com	11D 02h 45m 32s		100 Group (100 Group) is a 100% subsidiary of the 100 Group. On behalf of the State of

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.

Gartner
Peer *Insights*.

4.9 ★★★★★

AICPA
SOC 2
TYPE II
Thogopass™

[Sign Up for a Free Trial →](#)



flare.io

hello@flare.io