flare

Data Extortion Ransomware & The Cybercrime Supply Chain: Key Trends in 2023

Table of Contents

Data Extortion Ransomware & The Cybercrime Supply Chain: Key Trends in 2023

By: Eric Clay, Security Researcher

Introduction

In 2019, the nature of ransomware fundamentally changed. Ransomware operators are traditionally associated with denying the availability of IT infrastructure by encrypting systems and then extorting the victim. 2019 saw the advent of a new tactic; the ransomware group Maze began stealing data prior to encryption and then blackmailing victims by threatening to release sensitive data and files, jeopardizing both confidentiality and availability of data.

This Flare research report will focus on a new and potentially dangerous trend: the rapid adoption of data extortion tactics by ransomware groups and affiliates. To do this, we will begin by examining how ransomware groups operate within the framework of the broader cybercrime ecosystem. We will then carefully review data from thousands of double and triple extortion ransomware attacks to answer key questions, including how trends around data extortion attacks are changing over time, which groups represent the most significant threat, and which industries are most affected. Finally, we will provide concrete, evidence-based recommendations for cyber threat intelligence (CTI) teams, red teams, blue teams, and security leadership.

This report will be split into three sections, each designed to contextualize and help security teams better understand the threat from ransomware groups and affiliates. SalesIntel provided data to better understand victims in this report.

Section 1 focuses on the role of ransomware groups and affiliates in the broader cybercrime ecosystem. This section will examine evidence of how ransomware groups gain initial access to systems, what they do with that access, and the anatomy of an attack.

Section 2 provides a detailed analysis of data collected from more than 3,000 ransomware leaks to examine key trends related to ransomware.

Section 3 offers actionable, evidence-based recommendations for CISOs, CTI teams, and security operations teams on how to reduce the risk of ransomware.

Terms and Definitions

- **Data Extortion:** Refers to a ransomware tactic in which the ransomware operator exfiltrated data and threatens to publish it if the ransom is not paid.
- **Double Extortion Ransomware:** Refers to tactics in which two methods of extortion are used (for example, data extortion and encryption).
- **Triple Extortion Ransomware:** Refers to ransomware events in which at least three separate extortion methods are used to try and force the victim to pay, for example, encryption, data extortion, and third-party notification).
- **Ransomware Group:** Refers to an organized, criminal group focused on ransomware creation, distribution, and extortion.
- **Ransomware Affiliate:** Refers to an outside party that partners with a ransomware group and shares in potential profits.
- **Ransomware Blog:** Refers a website on Tor run by a ransomware group where victim data is published.
- **Dedicated Leak Site (DLS):** refers to a website/hidden service where the ransomware operators publish the stolen data. More advanced groups will usually maintain a blog AND a DLS.

Executive Summary

- Ransomware attacks involving data extortion have increased at an annualized rate of more than **112% in 2023.**
- Manufacturing, Information Technology, and Professional Services are the most targeted industries.
- LockBit, Alphvm, CL0P, and BianLian remain the most active groups in 2023, with LockBit eclipsing all other groups by sheer number of ransomware extortion posts.
- Ransomware groups are very likely using infostealer logs containing single sign-on (SSO) and active directory federation service (AD FS) credentials as a vector of attack.
- Ransomware groups continue to proliferate, with dozens of active groups, many with affiliate programs enabling the "democratization" of ransomware.

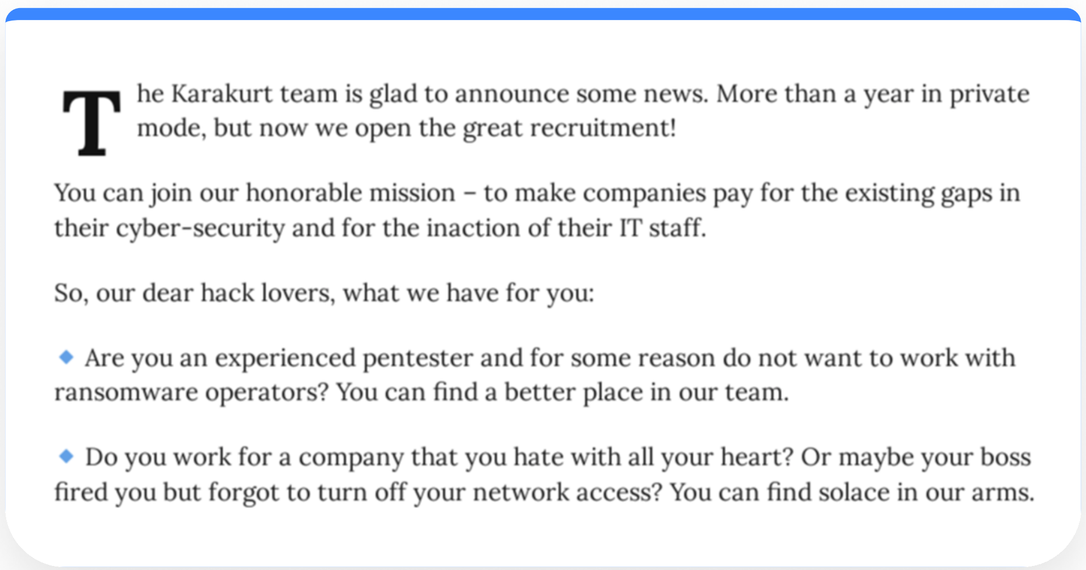
Section 1: Ransomware Groups, Data Extortion, and Placing the Ransomware Economy in the Broader Cybercrime Ecosystem

It is impossible to understand how ransomware groups operate without understanding their role in the broader cybercrime ecosystem. Groups do not operate in a vacuum; instead, they are provided with initial access to corporate IT environments, credentials, and cookies for SSO applications, and ready-made infrastructure for distribution. We will examine each leg of the ransomware support infrastructure in turn.

Ransomware Groups and Ransomware Affiliates

Understanding the sharp distinction between ransomware groups and ransomware affiliates is necessary to contextualize their place in the broader cybercrime ecosystem. Ransomware groups are self-sufficient entities that take different organizational forms.

In many cases, they are organized similarly to corporations, with clear hierarchies and role specializations. Some ransomware groups, such as Karakurt, operate entirely self sufficiently, creating and distributing ransomware, while also collecting ransoms.



The Karakurt team is glad to announce some news. More than a year in private mode, but now we open the great recruitment!

You can join our honorable mission – to make companies pay for the existing gaps in their cyber-security and for the inaction of their IT staff.

So, our dear hack lovers, what we have for you:

- Are you an experienced pentester and for some reason do not want to work with ransomware operators? You can find a better place in our team.
- Do you work for a company that you hate with all your heart? Or maybe your boss fired you but forgot to turn off your network access? You can find solace in our arms.

Ransomware group Karakurt's recruitment page

However, other groups have developed a different business model. Groups such as LockBit operate affiliate programs in which the group provides the ransomware to outside contractors who manage gaining initial access and infecting systems. This allows the groups to leverage economies of scale and role specialization, infecting more victims and increasing payouts. It also de-risks the group; for example, even if nine affiliates fail to carry out a substantial attack, the group can still profit from the successful 10th. This strategy also allows the group itself to focus on code and ransomware feature sets.

Infostealers, Dark Web Marketplaces, and Paid Telegram Channels

Infostealer malware and stealer logs represent one of the most underappreciated risks in modern cybersecurity programs. Infostealer variants such as RedLine, Raccoon, Aurora, Vidar, Titan, and others infect victim computers mainly through cracked software downloads, malvertising, and phishing emails. They then proceed to exfiltrate data from the infected device, including the browser fingerprint, which includes all the credentials saved on the browser along with active session cookies, credit card information, and information about the host.

This information is then packaged into log files, which are distributed on dark web marketplaces and cybercrime Telegram channels. Stealer logs represent a potentially massive access vector for ransomware groups. They:

- Are easily obtainable and given out freely on Telegram.
- Often contain access to corporate SSO applications, Active Directory (AD) environments, and remote desktop protocol (RDP).
- Represent a known vector that ransomware groups and affiliates have used to gain access to corporate IT systems.

We have also seen substantial evidence of initial access brokers (IAB) operating on the dark web forums Exploit and XSS utilizing stealer logs to gain initial access to corporate environments which are later resold for ransomware.

Key Fact: Flare's researchers identified 196,970 instances of AD credentials and 53,292 corporate SSO credentials in a sample of more than twenty million unique stealer logs. These credentials were leaked due to users downloading Infostealer malware onto their computers, which harvested AD and SSO credentials. AD environments represent a critical access point for ransomware threat actors. Many groups attempt to take over AD environments and de-privilege other administrators as a first step before exfiltrating files and beginning to encrypt documents.

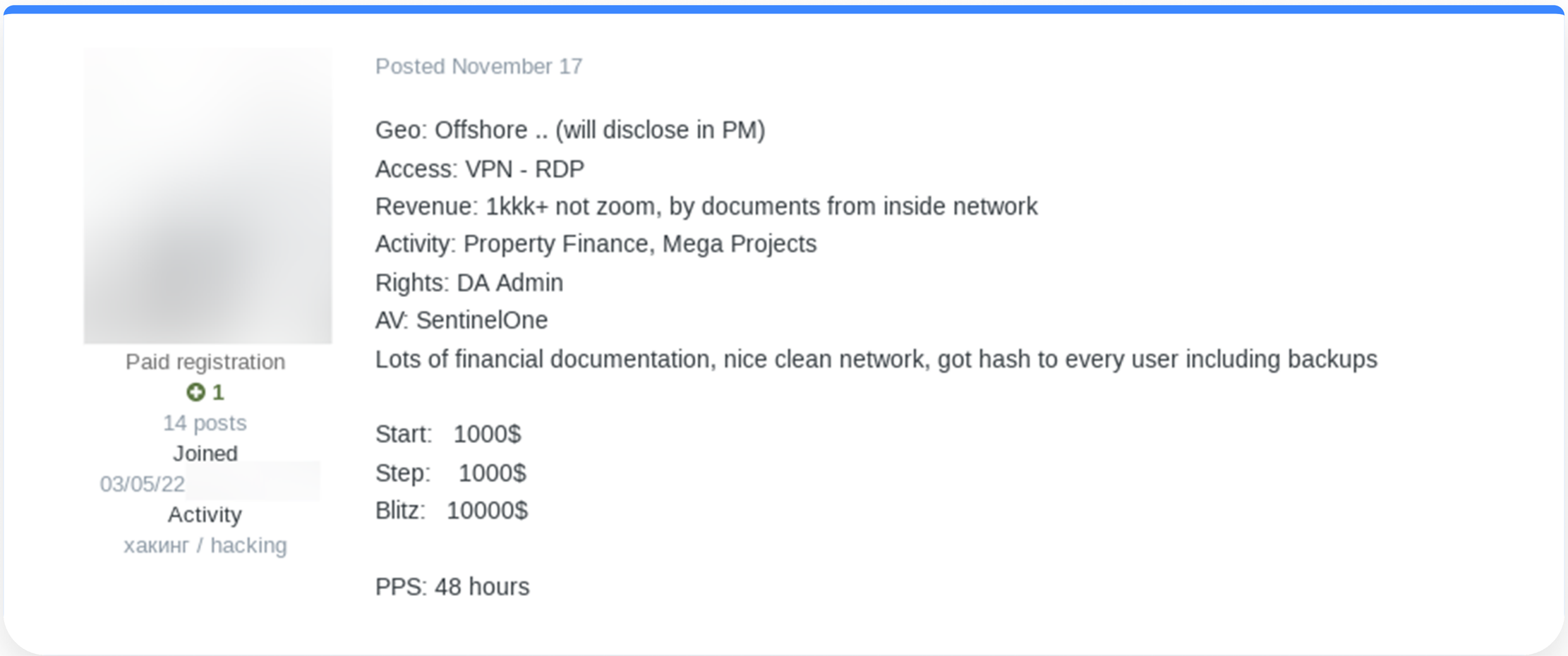
Malware as a Service and Cybercrime Infrastructure Vendors

Phishing, spear-phishing, and leaked credentials continue to represent one of the most common ways that groups gain access to privileged systems. Malware as a service (MaaS) and Phishing as a Service (PaaS) vendors on the dark web provide all the infrastructure and malware necessary to gain initial access, without the need for the ransomware operator to code infostealer malware or ransomware themselves. These vendors offer a range of services, including exploit kits, remote access trojans (RAT), and botnets, allowing cybercriminals to easily launch sophisticated attacks. By leveraging these services, ransomware operators can quickly and efficiently infiltrate networks and escalate their privileges.

Initial Access Brokers and Obtaining Privileged Access

IABs likely represent another key vector for ransomware groups and affiliates. IABs operate on the dark web forums Exploit and XSS; they specialize in gaining initial access to corporate IT environments which is later resold in an auction style format.

IABs don't post commonly, usually only one or two new listings per day. However, the listings are often high-quality and contain the exact type of access that ransomware operators need in order to compromise sensitive corporate networks and infrastructure. A typical post will include the number of hosts, anti-virus used by the victim, geography of the victim, and a "blitz" or buy it now price.



IAB post advertises selling access to financial documentation and an organization's network

Note the presence of "no backup servers" in the pictured initial access broker post. This likely indicates that the broker expects the access to be used for ransomware featuring encryption since in the context of cybercrime, backup and recovery is designed specifically to ensure data availability in the CIA triad.

Tor Ransomware Blogs

Tor ransomware blogs are run by ransom groups and used as a place to post updates to affiliates, advertise their affiliate programs, and most importantly post data leaks from victims who didn't pay the ransom. Sites like LockBit's blog create additional pressure for the victim by providing a countdown for the date that the victims information will be leaked, creating time pressure, and potentially alarming the victims third parties.

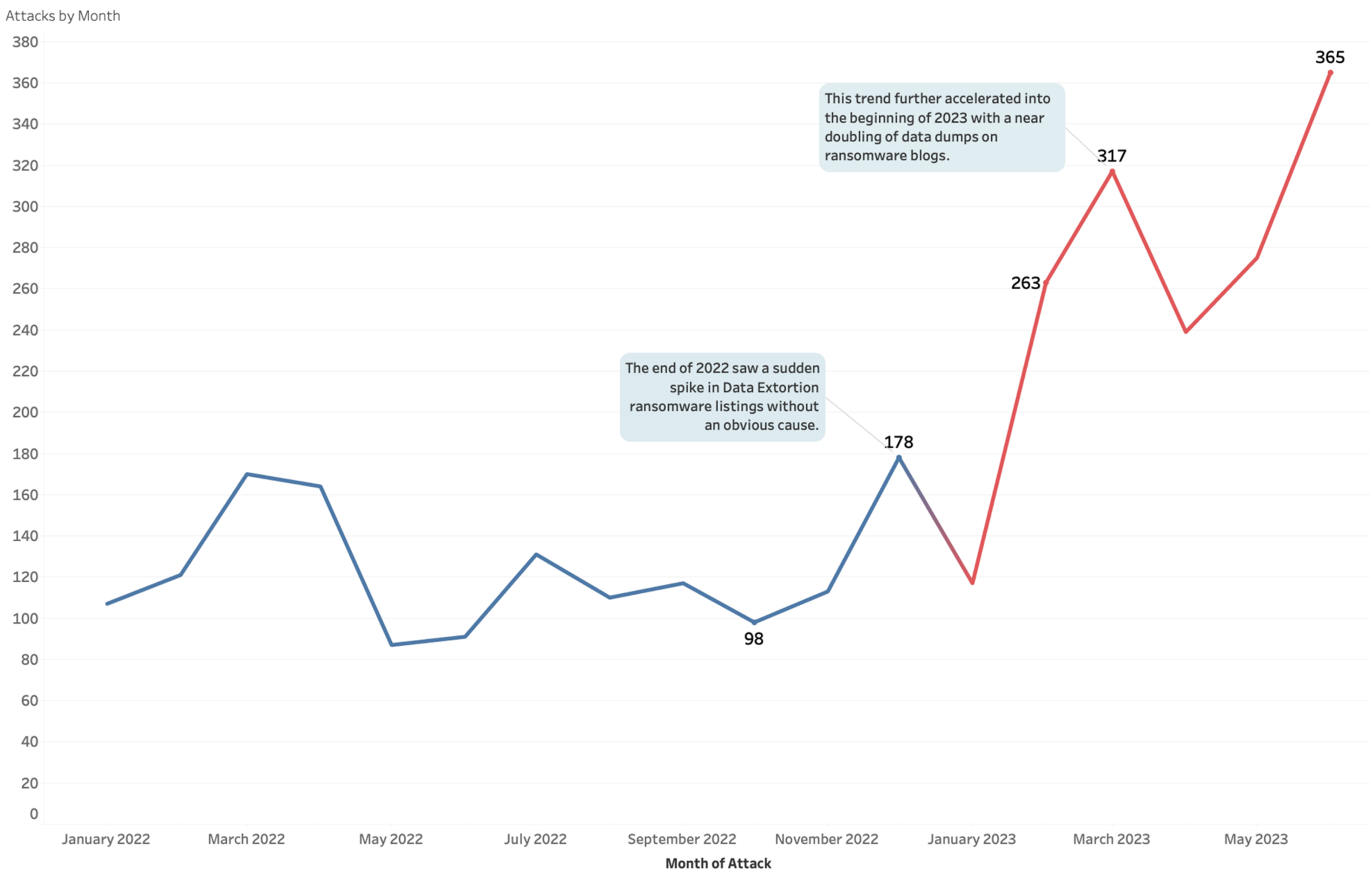
Ransomware blogs on Tor form a critical piece of ransomware group and affiliate infrastructure. Recently a few groups have tried posting leaked data on clear web sites, but quickly ran into problems keeping data available on clear web sites due to rapid corporate takedowns.

Section 2: Ransomware, Data Extortion, and the Explosive Growth of Organized Cybercrime

To better understand the challenge that ransomware poses to companies in 2023, Flare analyzed ransomware publications from more than 18 months of data. We looked at data from more than 80 ransom blogs comprising thousands of events to understand how ransomware is changing in 2023 and identify key trends that can help us understand where it is heading.

Data Extortion Ransomware is Growing Rapidly

Ransomware Attacks by Month (from January 2022 to July 2023)

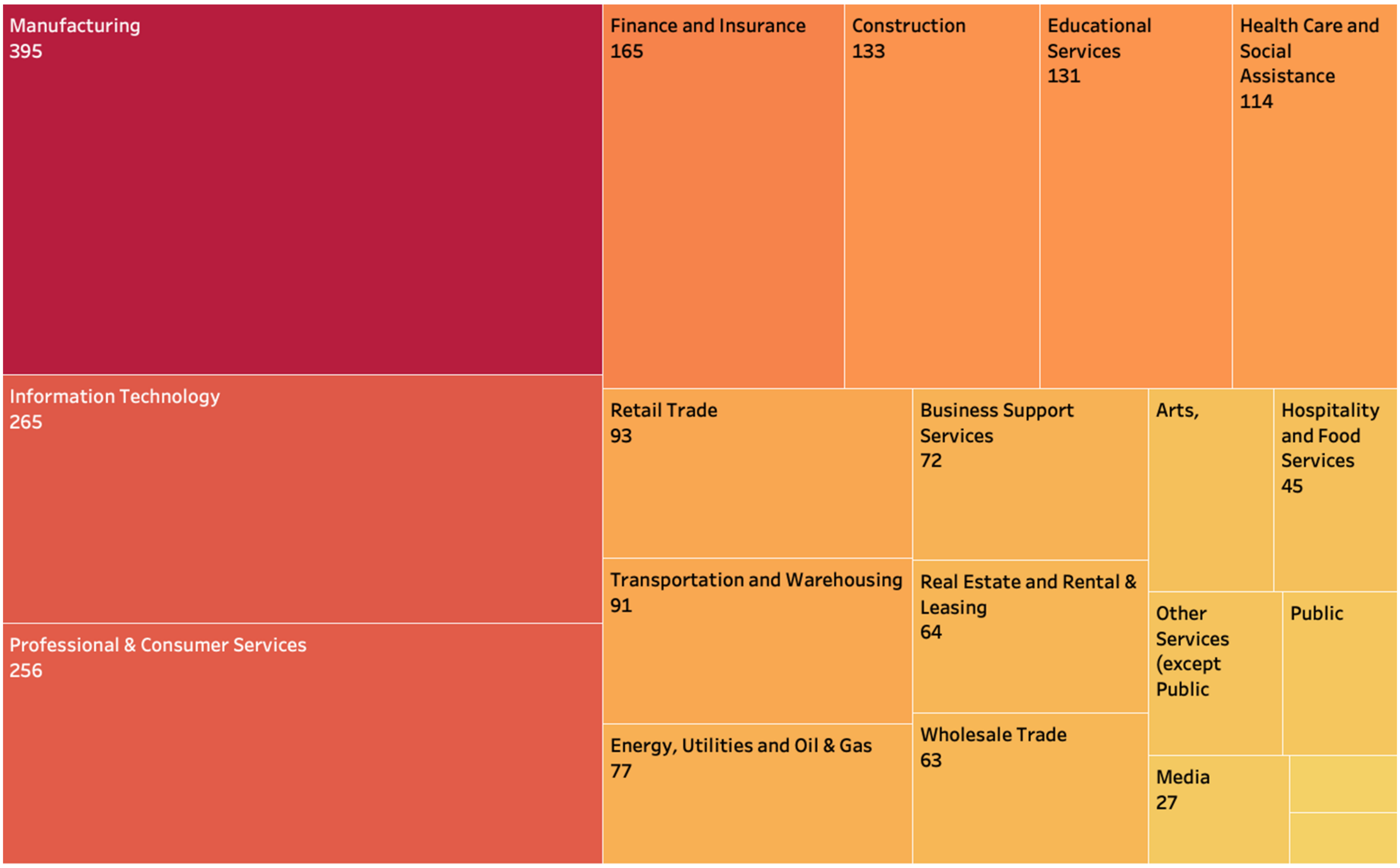


We begin our analysis by examining the dramatic increase in data extortion ransomware attacks in the past 12 months. After we account for the fact that our analysis runs to the end of July 2023, we find a 112% annualized increase in data extortion tactics in the past 18 months.

The dramatic increase in attacks does not paint a full picture. Ransomware groups and victims are not distributed evenly. Next, we will look at which groups are responsible for the most attacks, and which sectors are responsible for the most victims.

For organizations that we had a sector for, Manufacturing is by far the most likely sector to be victimized. Interestingly, this result diverges significantly from our recent analysis of IABs, in which manufacturing was the fifth most common sector to be victimized in the past three months.

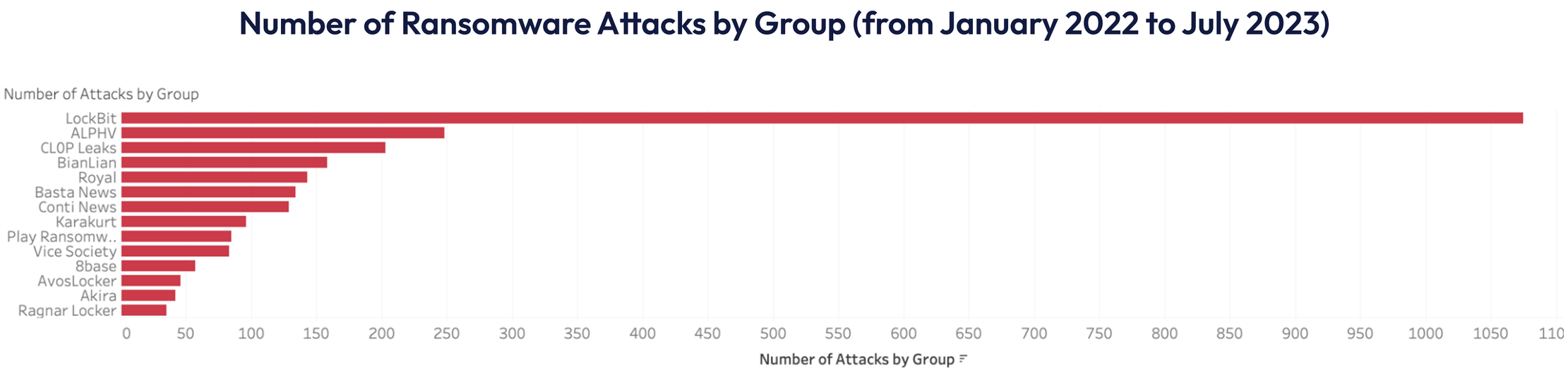
Number of Ransomware Attacks by Sector (from January 2022 to July 2023)



There are substantial differences in the industries that groups target. Manufacturing, Information Technology, and Professional and Consumer Services made the top of our list.

- **Information Technology:** 2021 and 2022 have seen a significant number of “supply chain” ransomware attacks in which MSSPs, and SaaS companies with privileged access to customer environments were targeted and used as a method to distribute ransomware.
- **Professional and Consumer Services:** Professional services encompasses organizations such as law firms, accounting practices, consultants and other types of firms that hold large amounts of highly sensitive client data. These organizations have a substantial incentive to pay ransoms to avoid compromising client data.
- **Finance and Insurance:** Financial services organizations are the fourth most attacked industry in our data set. Financial services companies hold some of the most sensitive possible data on both business and individual customers.

Next we analyzed which groups (and affiliates) are responsible for the majority of attacks. Unsurprisingly Lockbit came out dramatically ahead of every other group with more than 1,000 attacks over the time period studied.

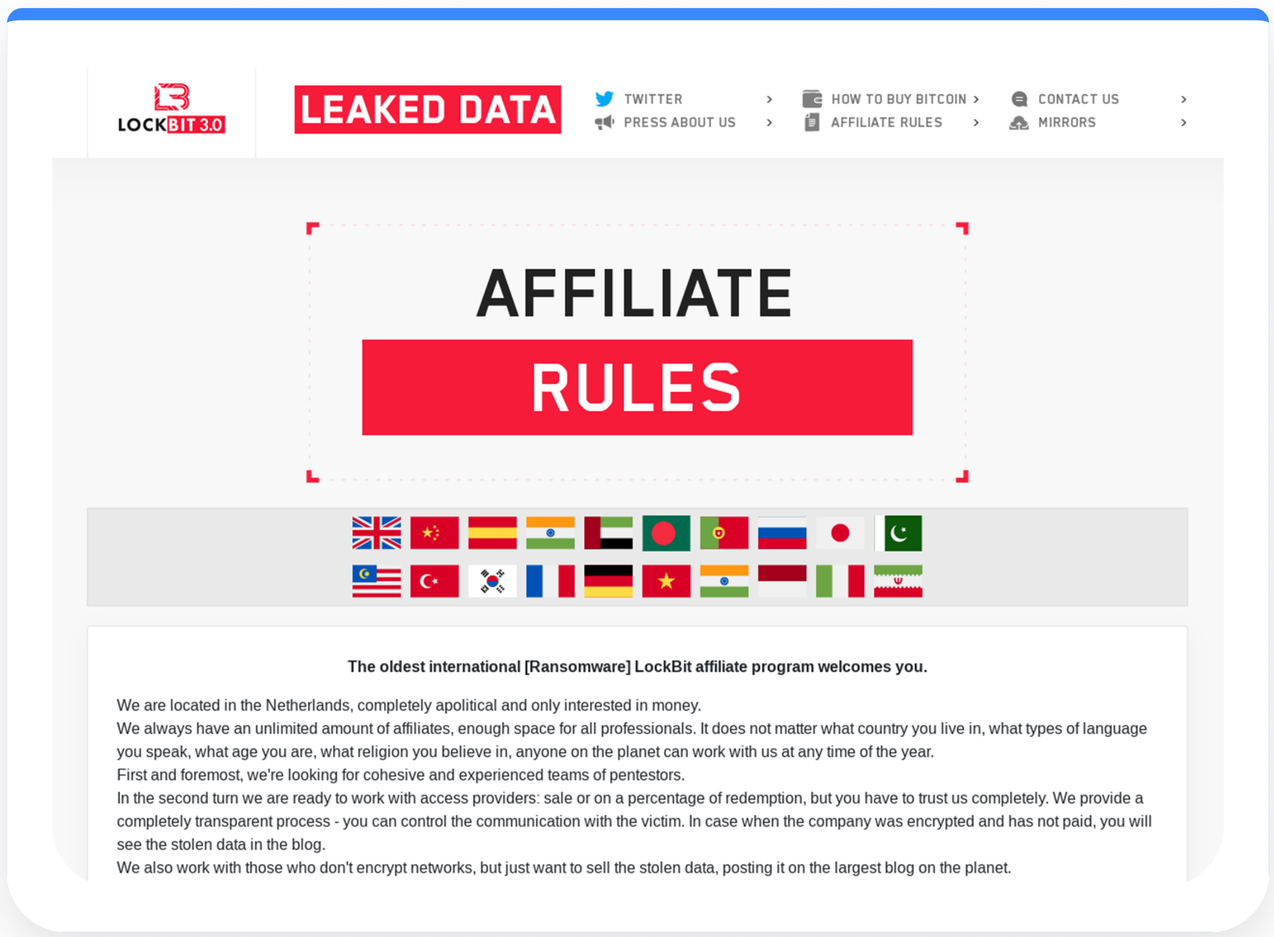


LockBit Ransomware as a Service Group

Lockbit emerged rapidly in late 2019, initially distributing ACBD ransomware before renaming themselves LockBit. They now have a notoriously ambitious affiliate program and nearly 100 affiliates working to compromise companies, and a highly functional ransomware blog where victim data can be easily published.

Lockbit's ransomware as a service offering has an easy "point and click" UI[1], enabling threat actors of all levels to effectively leverage it for distribution. In 2022 the group accounted for more than 20% of ransomware attacks in some countries, with tens of millions of dollars in damages.

LockBit has been responsible for numerous high-profile attacks, including on the City of Oakland, Italian Revenue Service, and the UK Royal Mail[2], causing significant financial losses and reputational damage to their victims. Their advanced techniques include leveraging zero-day vulnerabilities and employing social engineering tactics to exploit human vulnerabilities within organizations. This constant evolution and adaptability have made LockBit one of the most formidable and elusive ransomware groups in the cybersecurity landscape.



LockBit's Affiliate Rules webpage

[1]https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

[2]https://www.cpomagazine.com/cyber-security/cisa-alert-lockbit-ransomware-extorted-91-million-from-us-organizations/

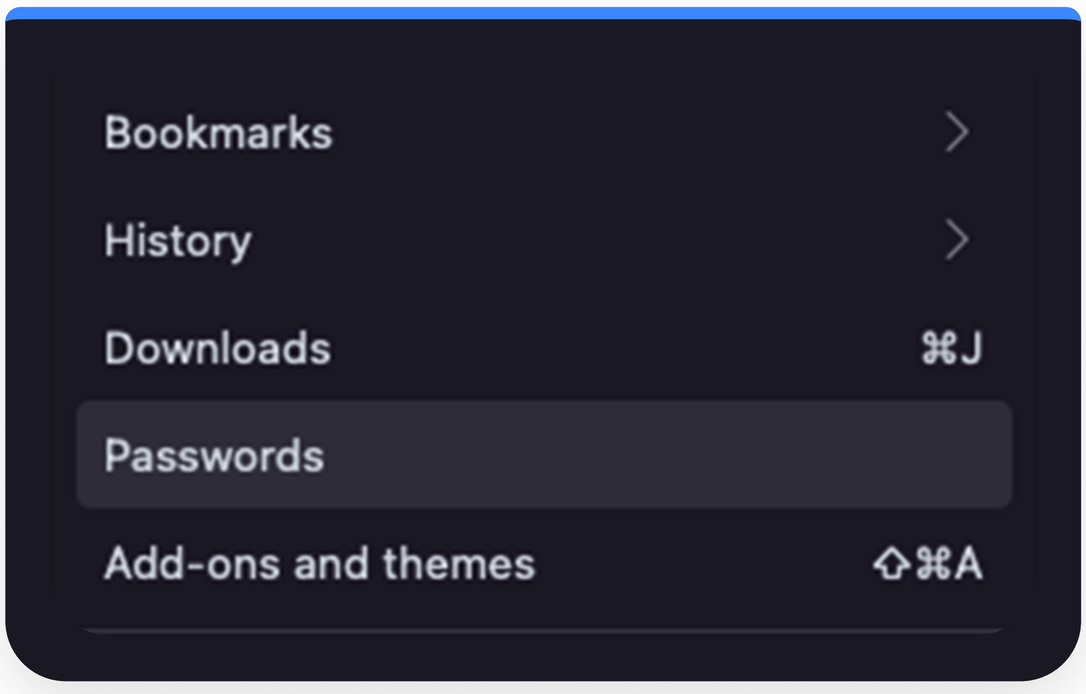
Section 3: Blue Teaming Recommendations

Ransomware groups exploit three primary vectors to gain access to organizations:

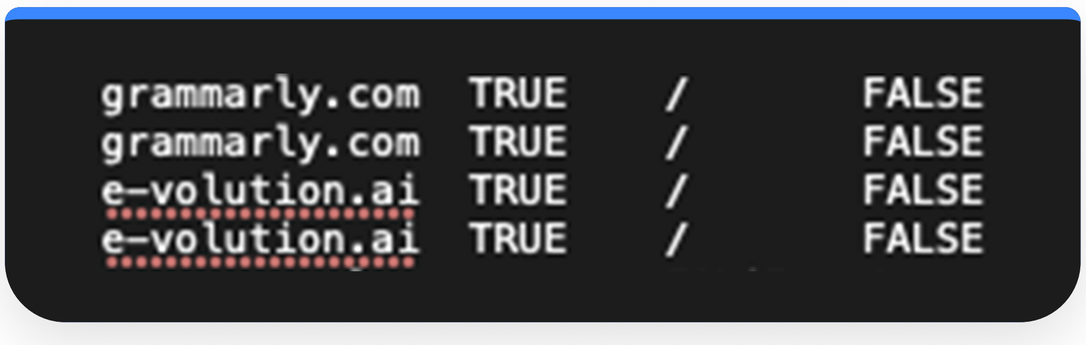
- Stolen Credentials
- Vulnerabilities
- Human Error

Stealer Logs and Leaked Credentials

Stolen credentials have long been considered a top vector for successful data breaches and ransomware attacks[3]. However, their importance has only increased with the advent of a class of RAT dubbed infostealer malware. Infostealers infect computers and steal all of the credentials saved in the browser, these credentials are then distributed across the dark web and Telegram. In many cases they contain active session cookies enabling threat actors to easily bypass 2FA and MFA controls.



Passwords in browser



Active cookie sessions

In addition, traditional leaked credentials also pose a significant threat. In many cases individuals reuse passwords across multiple services. If those services suffer a data breach and the individual has used the same credentials for RDP, VPNs, and corporate SaaS applications, this can serve as an easy entry point for ransomware operators. Typically once a group or affiliate has access to a network, they will attempt to move laterally to access AD at which point they privilege other users and begin stealing files.

[3] https://www.verizon.com/business/resources/reports/dbir/

Best Practices

- Ensure you have robust detection measures in place for stealer logs on Russian Market, Genesis Market, and public/private Telegram groups.
- Monitor for employees reusing passwords that have been breached and pay particular attention to employees that have reused the same password across multiple breaches.
- Monitor for stealer logs that contain specific access to RDP, VPN, and SSO credentials that could lead to a compromise.

About Flare

Flare is the proactive external cyber threat exposure management solution for organizations. Our AI-driven technology constantly scans the online world, including the clear & dark web, to discover unknown events, automatically prioritize risks, and deliver actionable intelligence you can use instantly to improve security. Our solution integrates into your security program in 30 minutes to provide your team with actionable intelligence and automated remediation for threats across the clear & dark web.

Want to learn about how Flare can support monitoring for ransomware activities?

Free Trial **Book a Demo**

flare.io

hello@flare.io