Emerging Threat: Defending Against 8base – Uncovering Their Arsenal and Crafting Responses

logpoint.com/en/blog/emerging-threat/defending-against-8base/

Anish Bogati August 23, 2023

Fast Facts

- Top 5 most active ransomware groups for the months of June and July 2023.
- Utilizes Phobos ransomware variant as their main payload.
- Specifically targeting medium and small-scale industries.
- Uses multiple malware families like SystemBC and SmokeLoader to achieve their target.

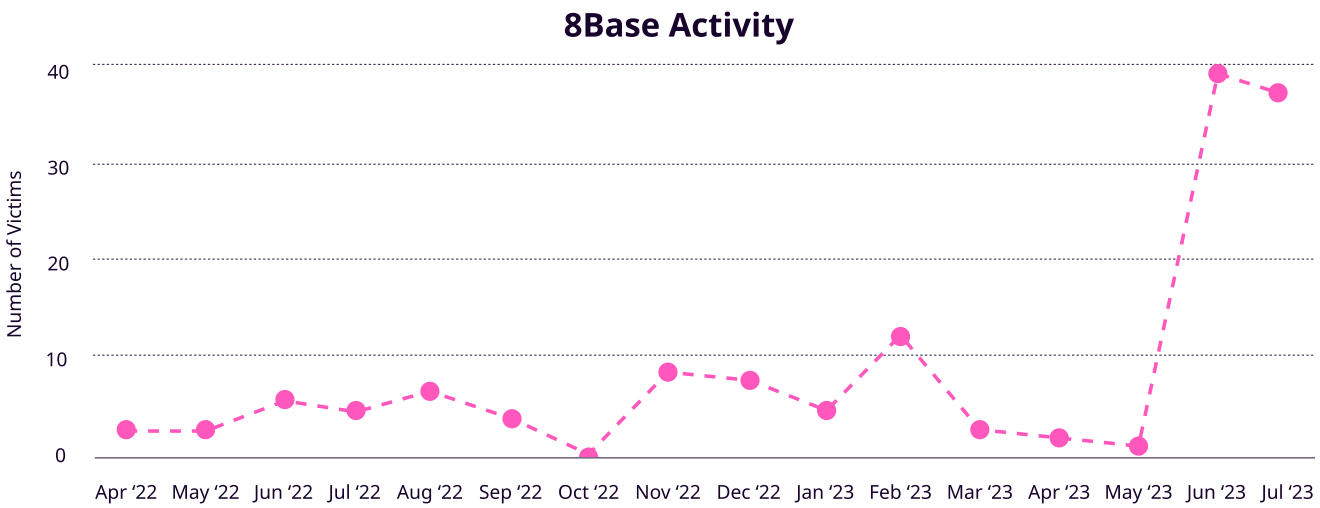
Anish Bogati
Global Services and Security Research

Download report

Background

The 8base ransomware group has established itself as a prominent player in the ransomware landscape, evident from the increasing number of victims whose data is leaked on their dedicated leak site. Their primary focus is targeting small and medium-scale industries, indicative of their specialized approach.

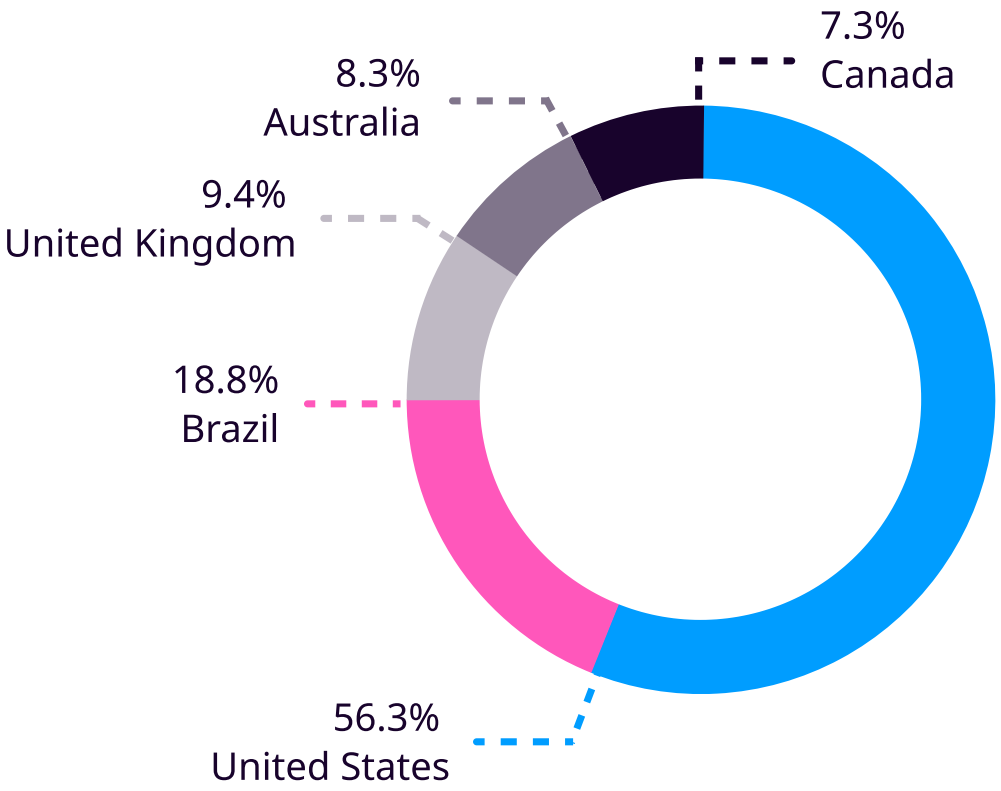
Although their activities began in March 2022, it was only after May 2023 that a substantial increase in group activities was observed, placing them among the top 5 most active ransomware groups since June 2023 on a monthly basis. This shift in their modus operandi became very noticeable after a tweet on May 14 by the group's Twitter account. Then the group started actively disclosing victim data from the preceding year and also of recent victims. We have continuously monitored data from ransomware.live, and the statistics are presented and interpreted in the chart below



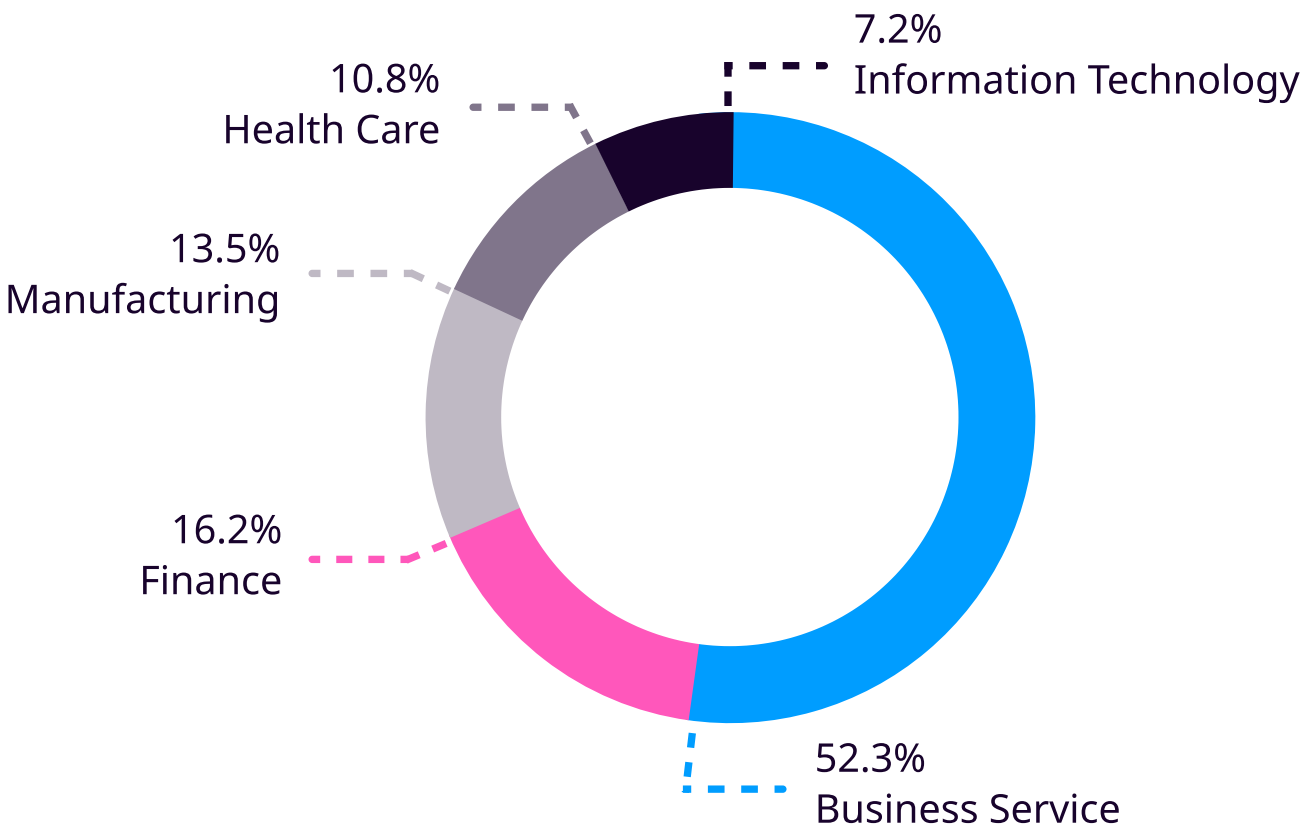
Although as of August 15th, there's no confirmation of the group creating or using their ransomware variant. The group is known to be using a customized version of the Phobos ransomware variant as their primary ransomware. According to VMware, SentinelOne, and Acronis, their data leak sites and communication style bear certain similarities with the RansomHouse group. Besides those, there is no precise evidence that provides the link between those groups.

Modes of Operation

Similar to many other ransomware families, 8base primarily targets organizations in the United States, followed by Brazil, the United Kingdom, Australia, and Canada, which are the top 5 most targeted countries.



The group has no specific targets as they are targeting multiple sectors such as Business Services, Finance, Manufacturing, Health Care, Hospitality Information Technology, etc. But Industries shown in the below images are the top 5 most targeted sectors by the group.



They are known to target victims via phishing as a means of initial access. SentinelOne has observed the group utilizing initial access brokers. According to Vmware, 8base have utilized SystemBC, to proxy their traffic, and create an encrypted C2 channel. The use of SmokeLoader has been observed to deploy the main ransomware payload in the victim systems. AhnLab has also provided information regarding the use of ExploitKit for the SmokeLoader delivery. After gaining access and elevating privilege, data exfiltration is performed which is later leaked in their Data Leak Sites.

Even though the group is around for more than a year not much is known about them. In the attached report, we delve deeply into the Tactics, Techniques, and Procedures (TTP) employed by adversaries, along with the respective capabilities of the malware they utilize. We have obtained malware samples and provided the analysis results, showcasing their capabilities. Following a comprehensive understanding of these capabilities, we've created and/or included existing detection rules to identify the various TTP used by the adversaries and have provided a playbook for automatic investigation and response.

**All new detection rules are available as part of Logpoint's latest release, as well as through the Logpoint Help Center.

Logpoint Emerging Threats Protection Service provides the service subscribers with customized investigation and response playbooks, tailored to their environment. Contact the Global Services team.

Download report