Conti vs. LockBit: A Comparative Analysis of Ransomware Groups

Published: 2022-06-27 · Archived: 2026-04-05 18:14:59 UTC

Ransomware

We compare the targeting and business models of the Conti and LockBit ransomware groups using data analysis approaches. This will be presented in full at the 34th Annual FIRST Conference on June 27, 2022.

By: Shingo Matsugaya, Matsukawa Bakuei, Vladimir Kropotov Jun 27, 2022 Read time: 5 min (1450 words)

Trend Micro has been monitoring the leak sites of multiple ransomware groups since November 2019 and continuously looking at the number and composition of organizations that have been victimized and whose information has been publicized by these groups. As a result of our research thus far, Continews article and LockBitnews article stand out in terms of their total numbers of affected organizations. Our goal with our research is to show how applying data analysis approaches to this data can give powerful understanding on the operations and perhaps even decision-making of these cybercriminals groups — a topic we will also be presenting on this week at the 34th Annual FIRST Conference in Dublin, with colleagues from Waratah Analytics. While some reports indicate the Conti brand is now offline, its scale continues to make it an excellent case study for these approaches.

When we rank the top 10 ransomware groups in terms of the number of organizations that had their data leaked (from November 2019 to March 2022), we see two clear leaders. In fact, Conti and Lockbit between them account for almost 45% of all incidents.

Rank	Ransomware group	Victim count
1	Conti	805
2	Lockbit	666
3	Maze	330
4	REvil/Sodinokibi	309
5	Pysa	307
6	DoppelPaymer	206
7	Egregor	197
8	Avaddon	184
9	NetWalker	178
10	Clop	119

Table 1. The top 10 ransomware groups in terms of the number of victimized organizations from November 2019 to March 2022

Here, by comparative analysis of the characteristics of the organizations victimized by these two major ransomware groups, we clarify their differences in attack tendencies.

Number of victimized organizations per month

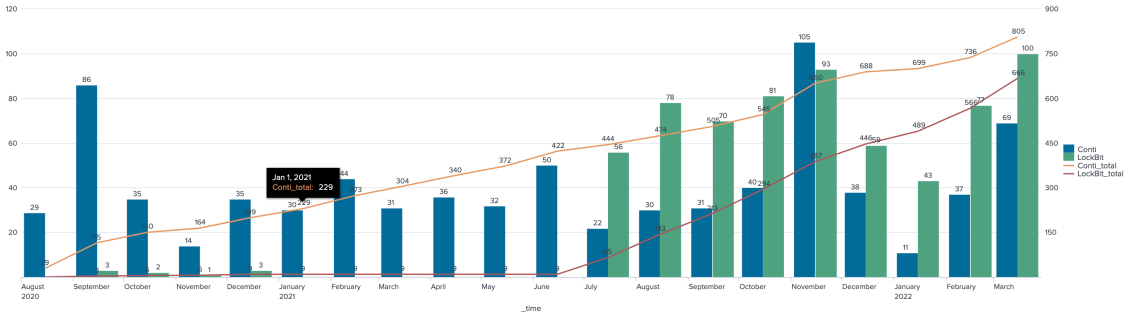

Figure 1. The monthly and cumulative numbers of organizations victimized by Conti and LockBit from August 2020 to March 2022

Since August 2020, there has been a large, stable number of organizations victimized by Conti, albeit with monthly increases and decreases. We have observed LockBit since September 2020, but the number of organizations victimized by the group per month has been very small, between one and three only. In addition, since January 2021, its original leak sites have been suspended and no victimized organizations have been reported. However, since its resumption of activity in July 2021, with the so-called LockBit 2.0, its number of victimized organizations has exceeded Conti's, making it the most active ransomware group. As a result, LockBit has been rapidly catching up in terms of the total number of victimized organizations, and as of March 2022, we have predicted that it will overtake Conti around August 2022 to become the largest ransomware group in terms of the total number of victimized organizations. However, with Conti likely having shut down in May 2022, or at least rebranding, it is almost certain that LockBit will overtake Conti sooner than expected.

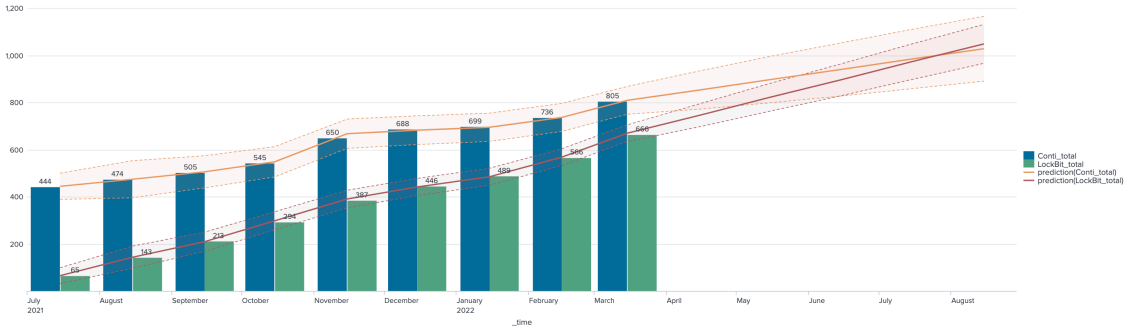

Figure 2. A predictive trend of Conti and Lockbit's future crossover point considering the numbers of organizations victimized by the two ransomware groups from July 2021 to March 2022 (prior to Conti's shutdown)

Victimized organizations by region

Figure 3. The regional distribution of organizations victimized by Conti (left) and LockBit (right) from November 2019 to March 2022

Looking at the regions where their victimized organizations are located, we see that there is a big difference between Conti and LockBit. For Conti, 93% of its victims are in North America and Europe, very much concentrated in these two regions. By comparison, 68% of LockBit's victims are in the same two regions. On the other hand, the areas of the victimized organizations are more dispersed for LockBit. We have observed many victimized organizations in Asia-Pacific, South/Latin America, and the Middle East, among others.

Comparing the regional distribution of organizations victimized by Conti and LockBit with the regional GDP distribution, LockBit is closer to the regional GDP distribution except for Asia-Pacific. Therefore, LockBit seems to be attacking specific regions more indiscriminately than Conti.

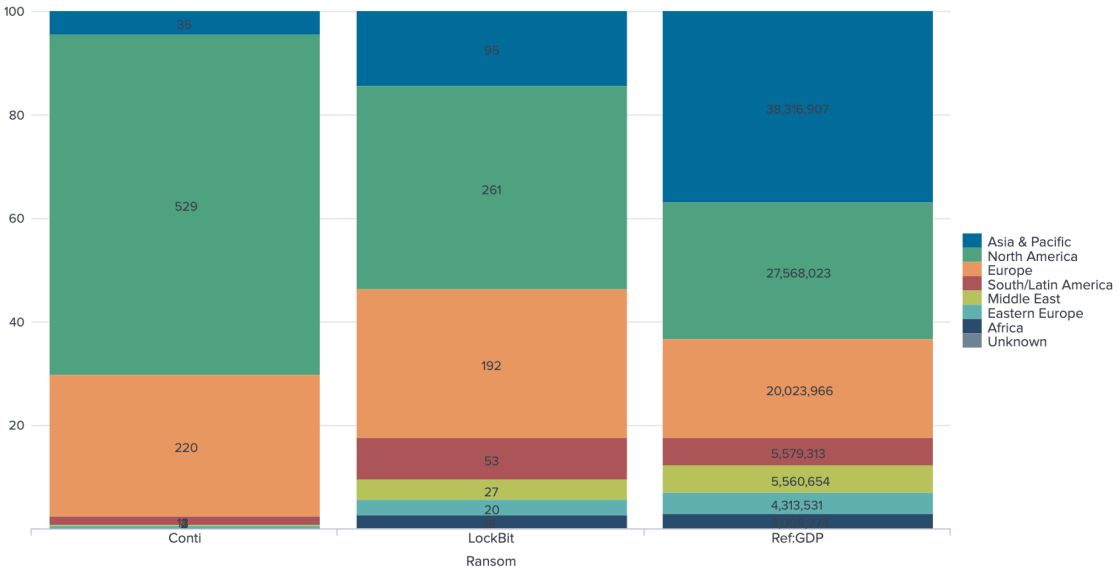

Figure 4. The regional distribution of organizations victimized by Conti (left) and LockBit (middle) from November 2019 to March 2022, and of GDP (right) as of March 2022

A closer look at the countries and regions of the victimized organizations in Asia-Pacific reveals that Conti has many victimized organizations in English-speaking countries such as Australia, India, New Zealand, and Singapore. LockBit's, on the other hand, are again more distributed in various countries.

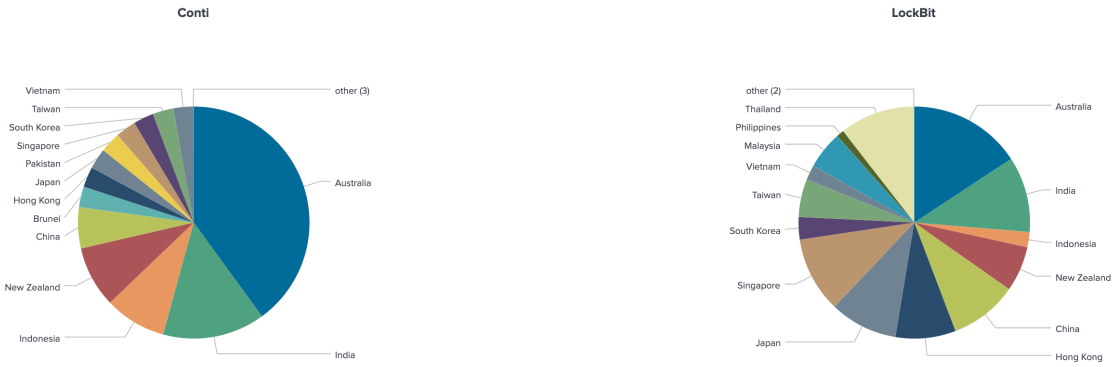

Figure 5. The distribution by country or region of organizations victimized by Conti (left) and LockBit (right) in Asia-Pacific from November 2019 to March 2022

Considering that the number of victimized organizations in Asia-Pacific is small for both Conti and LockBit compared to the GDP of the region, this suggests that local languages or alphabets might have been a barrier to these groups in attacking countries there, as in searching for confidential information to steal in an organization's network.

Looking at changes in the distribution of victimized organizations over time in a simple moving average, we see that Conti's attacks on organizations in Europe are on the rise.

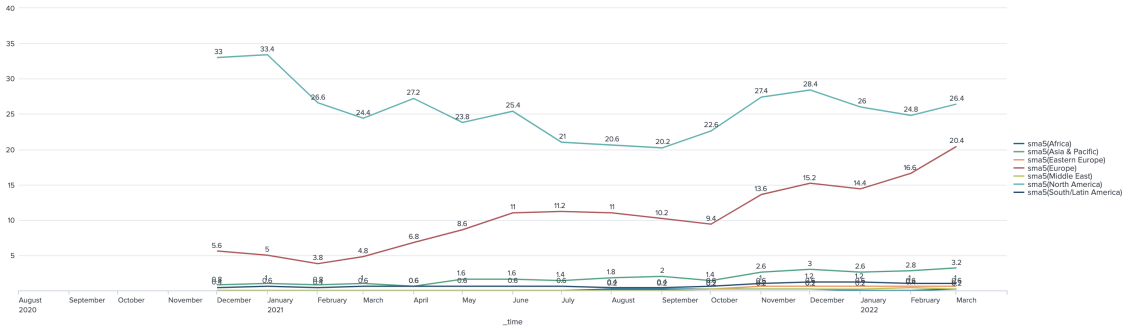

Figure 6. A simple moving average of the number of organizations victimized by Conti in each region from November 2020 to March 2022

In addition, closely looking at the regions other than the top two regions, we see that Conti's attacks on organizations in Asia-Pacific have been gradually increasing.

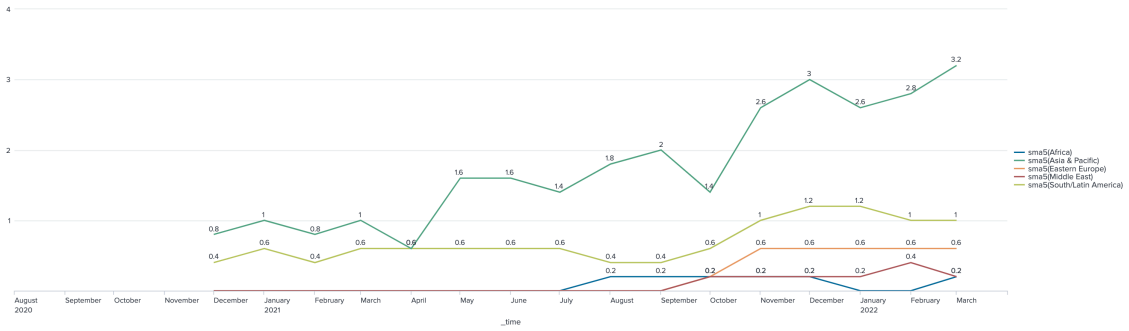

Figure 7. A simple moving average of the number of organizations victimized by Conti in each region, except North America and Europe, from November 2020 to March 2022

LockBit has also seen a slight increase in its attacks on organizations in Europe, but its distribution in each region has remained largely stable.

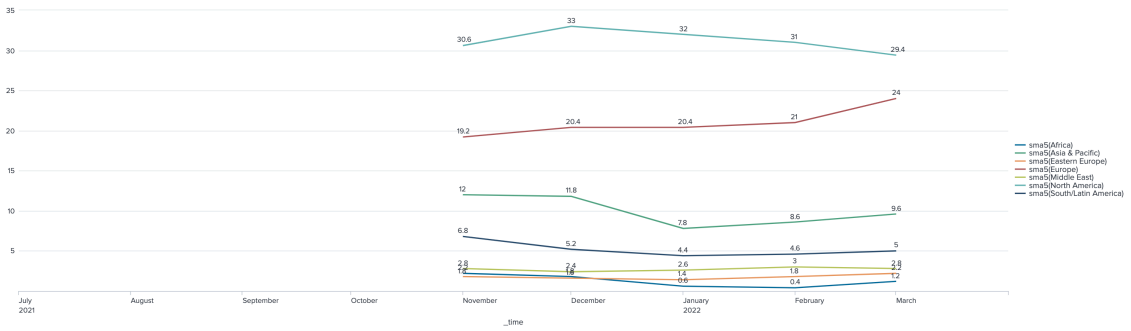

Figure 8. A simple moving average of the number of organizations victimized by LockBit in each region from November 2021 to March 2022

Victimized organizations by industry

Looking at the number of victimized organizations by industry, we see that both Conti and LockBit are distributed almost evenly across various industries (the top 15 industries are the same and in the same order), and it seems that there is no difference in their attack tendencies against industries. This indicates that they are not targeting specific industries.

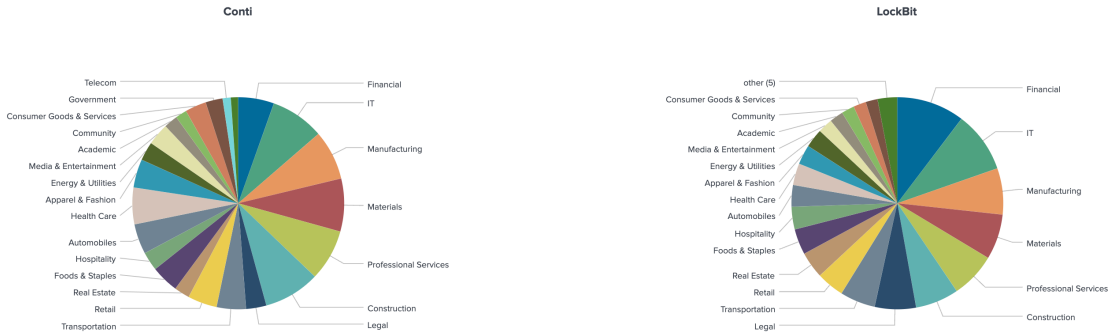

Figure 9. The distribution by industry of organizations victimized by Conti (left) and LockBit (right) from November 2019 to March 2022

Victimized organizations by number of employees

Looking at the number of victimized organizations by number of employees, we see LockBit has victimized more small organizations than Conti.

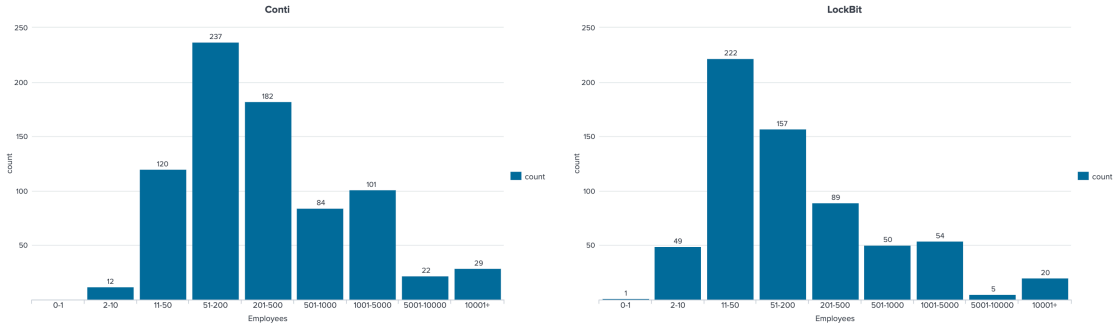

Figure 10. The distribution by number of employees of organizations victimized by Conti (left) and LockBit (right) from November 2019 to March 2022

Also, looking at the monthly number of changes in the moving average, LockBit has a stable ratio by number of employees, whereas Conti comparatively has a lot of variability and its attack tendency is not very stable.

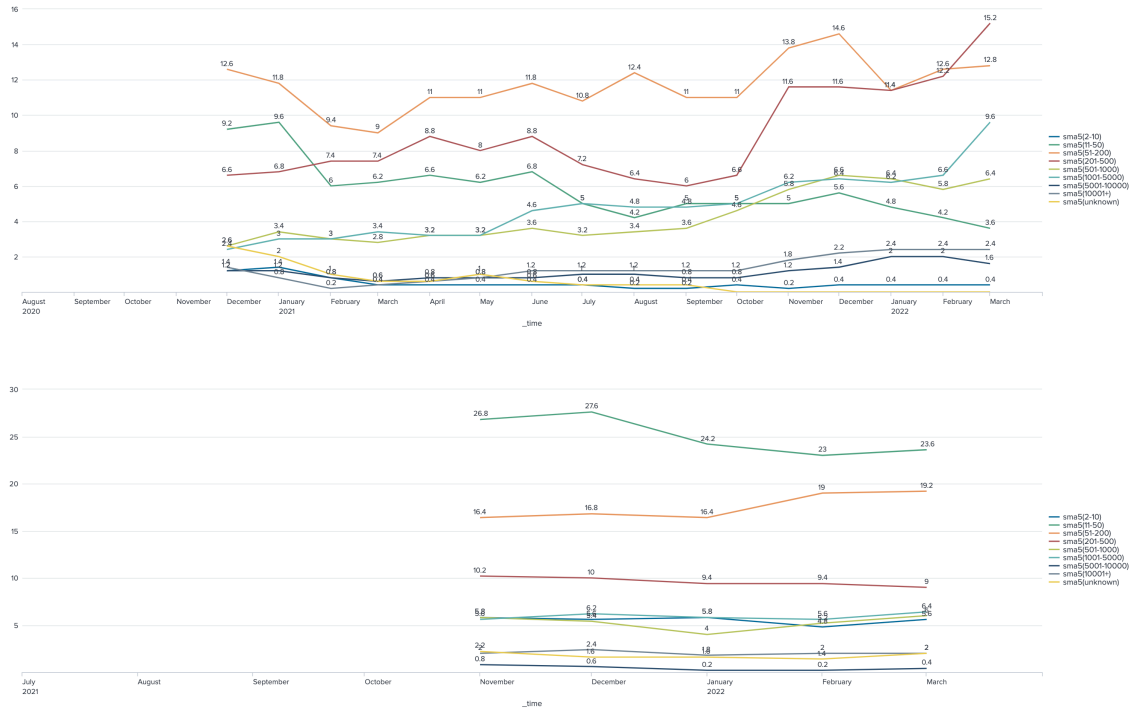

Figure 11. A simple moving average of the number of organizations victimized by Conti (top) from November 2020 to March 2022 and by LockBit (bottom) from November 2021 to March 2022 in each organization size in terms of number of employees

Conclusion

These characteristics visible from the data can be examined in greater depth by matching them with information provided by different threat intelligence sources. Conti, for example, has vowed not to target Russia's alliesnews article, such as former Soviet Union countries and China. It has also been reported that Conti prefers to target large organizations with more revenue and therefore more money to spare to earn more ransom.

LockBit, for its part, has stated that it selects targets only for financial motives without being influenced by political ties. It has also stated that its ringleader resides in Hong Kong. Since targeting an organization in one's

country or region of residence increases the risk of being investigated and arrested by the local police, it is practically a given that organizations in the country or region of residence should not be targeted from the viewpoint of the security of the attacker.

By applying data analysis approaches such as what we present here to other ransomware groups, and cross-checking the information from different threat intelligence sources with data leaks, it is possible to deeply analyze each group's characteristics. Furthermore, it is possible to gain deep insight into an attacker's targeting and business model and to quickly notice changes in the attacker's trends. This data, both current and predictive, can be invaluable for a range of people including network defenders looking to know where to invest for their security, insurers looking to understand risk, and law enforcement professionals.

More details and approaches about ransomware data analysis will be presented at the 34th Annual FIRST Conference in Dublin on June 27 by Vladimir Kropotov of Trend Micro and Eireann Leverett of Waratah Analytics.

Tags
