THREAT RESEARCH REPORT

Your Files Have Been Encrypted!

Ransomware Trends in 2022 and Why Threat Intelligence Matters

Drew Schmitt, Principal Threat Intelligence Analyst
GuidePoint Research and Intelligence Team (GRIT)

GUIDEPOINT
SECURITY

Introduction 3

Research Methodology 3

Starting with Some Educated Guesses 4

Hypothesis 1: The Ukraine/Russia conflict will result in a slowdown of ransomware operations 4

Hypothesis 2: Significant information leaks from ransomware groups should result in a notable reduction in operational capabilities 4

2022 Ransomware Trends 5

Some Groups Post More Victims Than Others, but All Groups are Dangerous Adversaries 5

Location, Location, Location 6

So What About Industry Verticals? 7

How Often are Victims Being Posted? 9

Ransomware Case Studies 10

Case Study One: 2022 Russian Invasion of Ukraine 10

Conti's Messaging Around the Ukraine/Russia Conflict 11

Conti Ransomware Trends During the Ukraine/Russia Conflict 12

Lockbit's Messaging Around the Ukraine/Russia Conflict 14

Lockbit Trends During the Ukraine/Russia Conflict 15

Ukraine/Russia Case Study Conclusions 17

Case Study Two: 2022 Conti Ransomware Leaks 17

Conti Leaks Case Study Conclusions 18

Overall Ransomware Conclusions 19

And Finally... Why Threat Intelligence Matters 20

What is Threat Intelligence Anyway? 20

Operationalizing Threat Intelligence 20

Have a Platform That You Can Control 21

Automate and Orchestrate Where Possible 21

View Your Attack Surface from the Attacker's Perspective 22

Have Eyes and Ears on the Dark Web 22

This is Why Threat Intelligence Matters 22

Introduction

2022, like years previous, continues the trend of ransomware being one of the most impactful and prolific threats that public and private sectors face on a daily basis. Events such as the Ukraine/Russia conflict and Conti Ransomware Group Leaks have added some complexities to the cyber landscape, and many have speculated how these events could impact the ransomware world. In this report, we will examine current ransomware trends as the first quarter of 2022 comes to a close. We'll leverage case studies based on two of the most prevalent ransomware groups of 2022 to determine what impacts international activities, such as the Ukraine/Russia conflict, have on ransomware groups' ability to cause damage and extort victims through their use of ransomware and leak sites.

Finally, based on our review of the 2022 trends and impacts of external events, we discuss why threat intelligence matters to organizations in all industry verticals, and how leveraging an effective threat intelligence program could be one of the most beneficial additions to your cybersecurity strategy in 2022.

Research Methodology

As part of our research methodology, we dusted off our 8th-grade science textbooks and reacquainted ourselves with the scientific method. All joking aside, we did leverage the scientific method to ensure that we had a data-driven approach to analyzing ransomware trends and the impacts that international events such as the Ukraine/Russia conflict might produce. From hypothesis, all the way to conclusions, we let the data dictate the outcomes, versus trying to confirm a hypothesis.

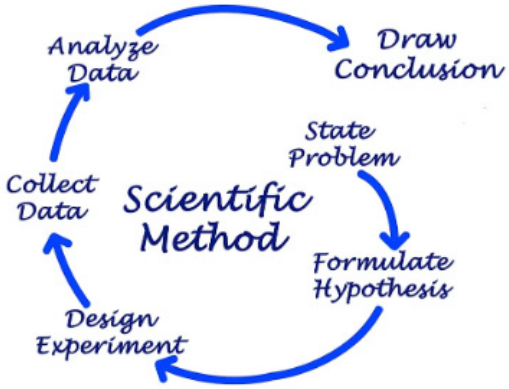

Figure 1: The Scientific Method

There are a couple of caveats we would like to spotlight regarding the data leveraged for this research to ensure appropriate context for interpretation and analysis.

1. **Our data set was derived from publicly available ransomware data collected from ransomware leak sites. No proprietary data sets were used for this analysis.**

Leak sites are leveraged by ransomware groups to extort their victims through the threat of releasing sensitive data. If you have ever interacted with ransomware leak sites in the past, you know there is an inherent level of volatility associated with them. The leak sites change based on victim negotiations, scrapers temporarily go out of date, and sometimes leak sites go offline. Additionally, these sites only account for victims that were published, and do not account for the multitude of companies that make contact and pay ransoms to prevent publication. All these factors might contribute to some level of error with respect to the data collected, so if there are some discrepancies between your data set, this could be why.

We also chose to go this route since it is the most widely available data set of published victims. To further explore the impacts of world events on how ransomware groups operate, we welcome and encourage other researchers to use this report as a jumping-off point, or reach out and collaborate to continue and enhance the research we've already performed.

2. **Our research considered the rebranding, stagnation, and incorporation of new ransomware groups as a constant from year to year**

Ransomware groups frequently go through rebranding processes, become stagnant for a multitude of reasons, and new ransomware groups continue to emerge on a regular basis. Our research considered this variation in actively posting ransomware groups as a constant from year to year and did not specifically investigate or analyze factors that influence the rates at which ransomware groups rebrand, become stagnant, or new groups emerge.

3. **Our analysis focused on data obtained from public ransomware leak site postings from January 1, 2022, to March 27, 2022.**

Although the primary focus of our analysis was on data obtained between January 1, 2022, and March 27, 2022, we also included data spanning the entirety of 2021 for ransomware groups we track. It is possible that some victims may have been removed by the time we started scraping the site and could have introduced a small margin of error into our data set.

Starting with Some Educated Guesses

At a very high level, our research began with the premise that ransomware is subject to influences from external events, which will have an effect on the rate at which a ransomware group's operations can be conducted, and/or the success of that ransomware group's operations. We decided to review ransomware trends through the lens of the Ukraine/Russia conflict and specifically focused on two hypotheses to drive our analysis.

Hypothesis 1: The Ukraine/Russia conflict will result in a slowdown of ransomware operations

Many ransomware groups are suspected to operate within eastern Europe or Russia, precisely where the Ukraine/Russia conflict is taking place. Additionally, many ransomware groups are suspected to be supported by, or at least not hindered by, the Russian government. With these factors considered, we hypothesize that due to the large-scale conflict, including major cyber components leveraged by the Russian government, occurring in the region, there will be a slowdown in the operational tempo of large ransomware groups.

Hypothesis 2: Significant information leaks from ransomware groups should result in a notable reduction in operational capabilities

Ransomware groups have been leveraging exfiltrated data for extortion purposes for one primary reason: information leaks are devastating to organizations. In many cases, leaked information provides damaging insight into how organizations operate and provides unfettered access to sensitive data. Whether the impact is brand or operationally related, leaked data has an impact.

Beginning on February 27, 2022, the tables were turned on the Conti Ransomware Group when they suffered their second information leak in less than 12 months. A Twitter account known as @Contileaks began leaking critical information regarding the group's operations and source code. We speculate that this type of breach will have devastating effects on Conti's operations.

2022 Ransomware Trends

Ransomware trends in 2022 are a continuation of what was observed throughout 2021. Plainly stated, ransomware continues to be a high-stakes threat for all organizations regardless of sector or industry vertical. At the time we conducted our analysis, there had already been over 600 victims across a wide variety of industry verticals, which were publicly posted to ransomware leak sites across 40 different ransomware groups.

Some Groups Post More Victims Than Others, but All Groups are Dangerous Adversaries

When reviewing the data associated with publicly posted ransomware victims from 2022, there were some groups that stood out immediately amongst the others. Lockbit, Conti, Hive, AlphV, and Karakurt accounted for nearly ⅔ of all publicly posted ransomware victims that we track.

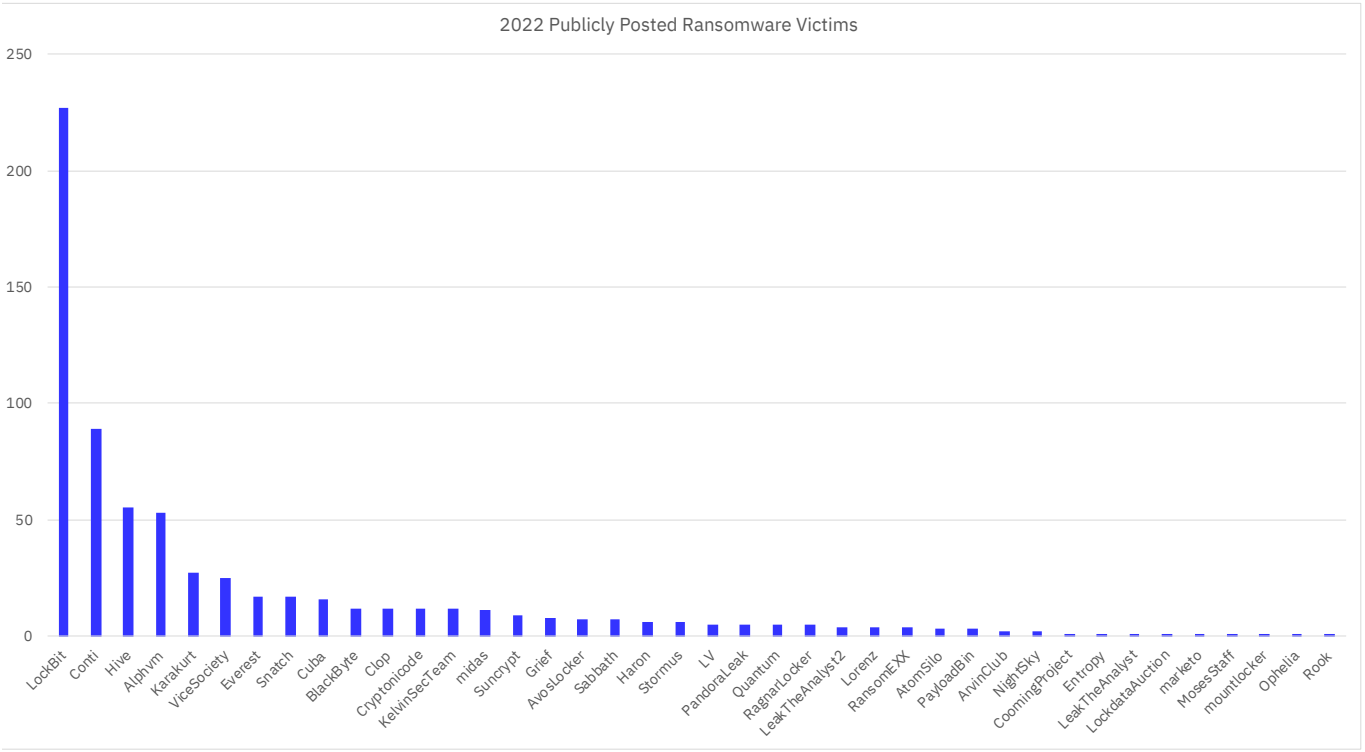

Figure 2: 2022 Publicly Posted Ransomware Victims

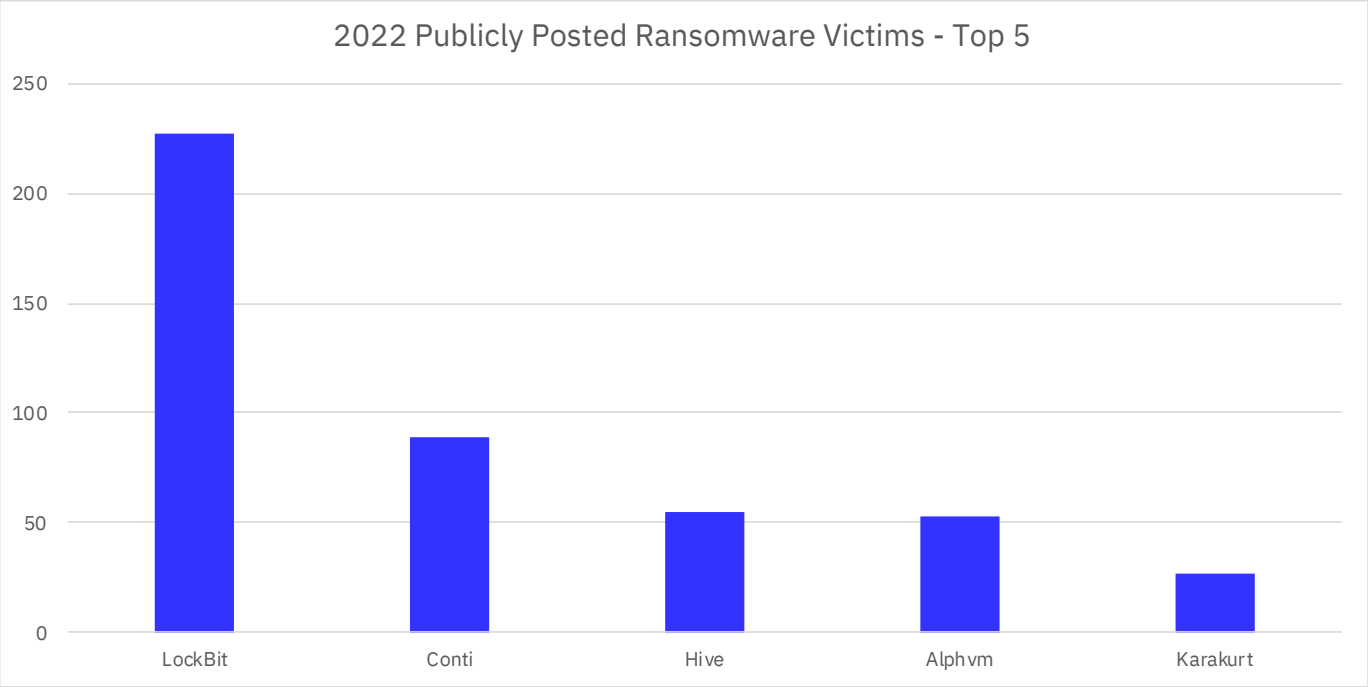

Figure 3: Top Five Ransomware Groups with Publicly Posted Victims

Anecdotally, not making the top five does not mean that other groups are not as dangerous. For instance, we have covered the Cuba Ransomware Group extensively in multiple published blogs[1][2] and demonstrated how they can effectively use critical vulnerabilities to gain access to victim organizations for ransomware attacks.

Location, Location, Location

Ransomware groups are known for capitalizing on opportunities presented by vulnerable organizations and their IT infrastructure. Additionally, ransomware groups, much like any eCrime group, are financially motivated and pursue targets where their efforts will be most rewarded with the cryptocurrency of their choice. Out of all publicly posted victims across all tracked ransomware groups, the United States accounted for 39% of victims, down from 55% in Q1 2021, while the next highest country, the United Kingdom, only accounted for 7% of the total posted victims. Outside of the top 10 countries with the most posted victims, the number of posted victims drops dramatically.

[1] https://www.guidepointsecurity.com/blog/using-hindsight-to-close-a-cuba-cold-case/

[2] https://www.guidepointsecurity.com/blog/a-ransomware-near-miss-proxyshell-a-rat-and-cobalt-strike/

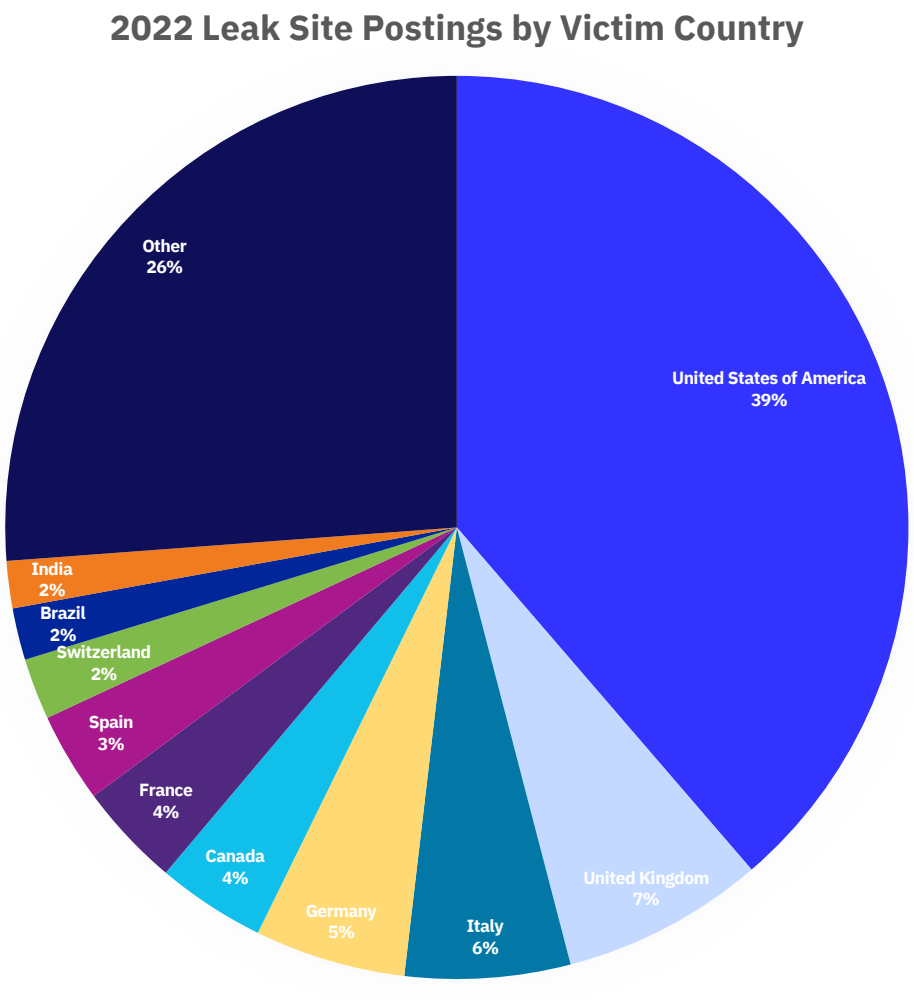

Figure 4: Leak Site Postings by Victim Country

Although there are a wide variety of countries and regions with victims that have been publicly posted as a victim of a ransomware extortion scheme, the trends indicate that western countries are affected more frequently than others. It is also very clear that countries with suspected ties to ransomware groups, including former Soviet Union countries, China, and North Korea, have far fewer victims than other countries.

So What About Industry Verticals?

Over the years, we have become accustomed to seeing certain industry verticals heavily represented in our statistics related to ransomware attacks. As 2022 progresses, we are tracking the same trends from 2021 and earlier, where many commonly observed industries are again topping the charts for publicly posted ransomware victims.

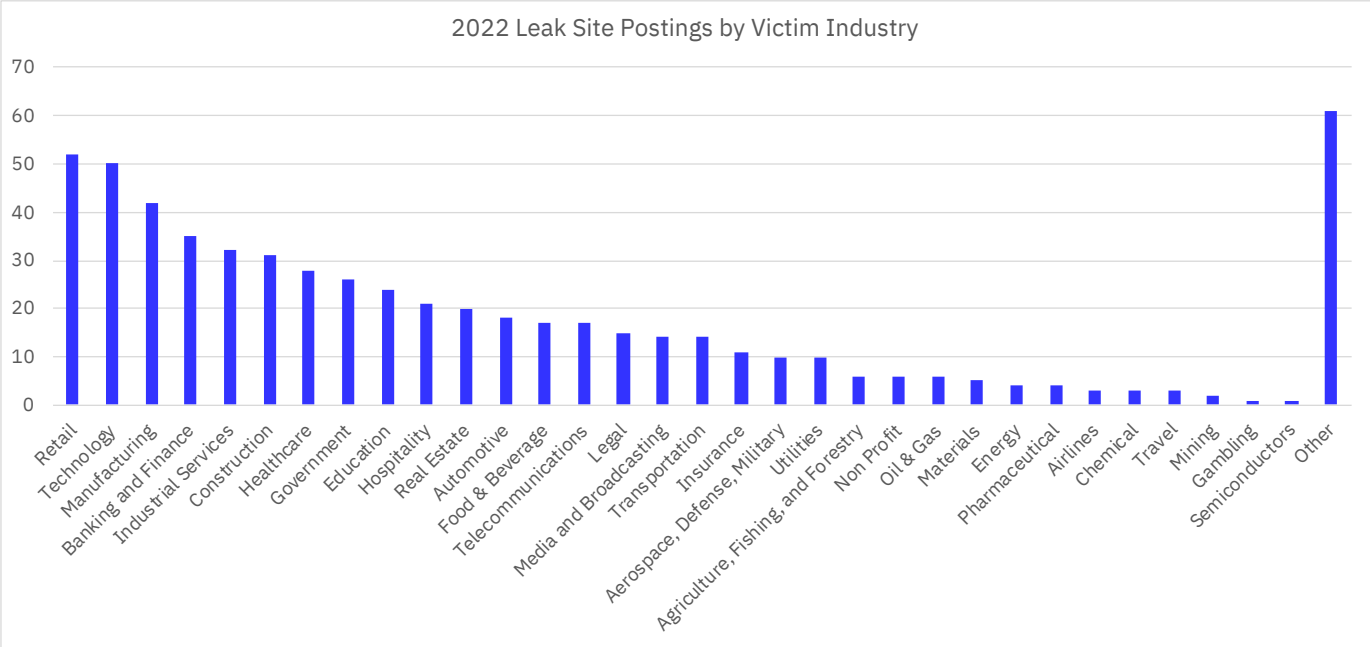

Figure 5: Leak Site Postings by Victim Industry

Since the ransomware attack on the Colonial Pipeline, there has been significant focus on ransomware attacks affecting critical infrastructure. Some critical infrastructure verticals such as oil & gas and energy appear to be less affected by ransomware based on publicly posted victims, although some speculate this is related to the backlash observed from the Colonial Pipeline attack. That being said, some critical infrastructure verticals such as Finance, Information Technology, and Healthcare continue to find themselves in the top 10 industry verticals affected by ransomware.

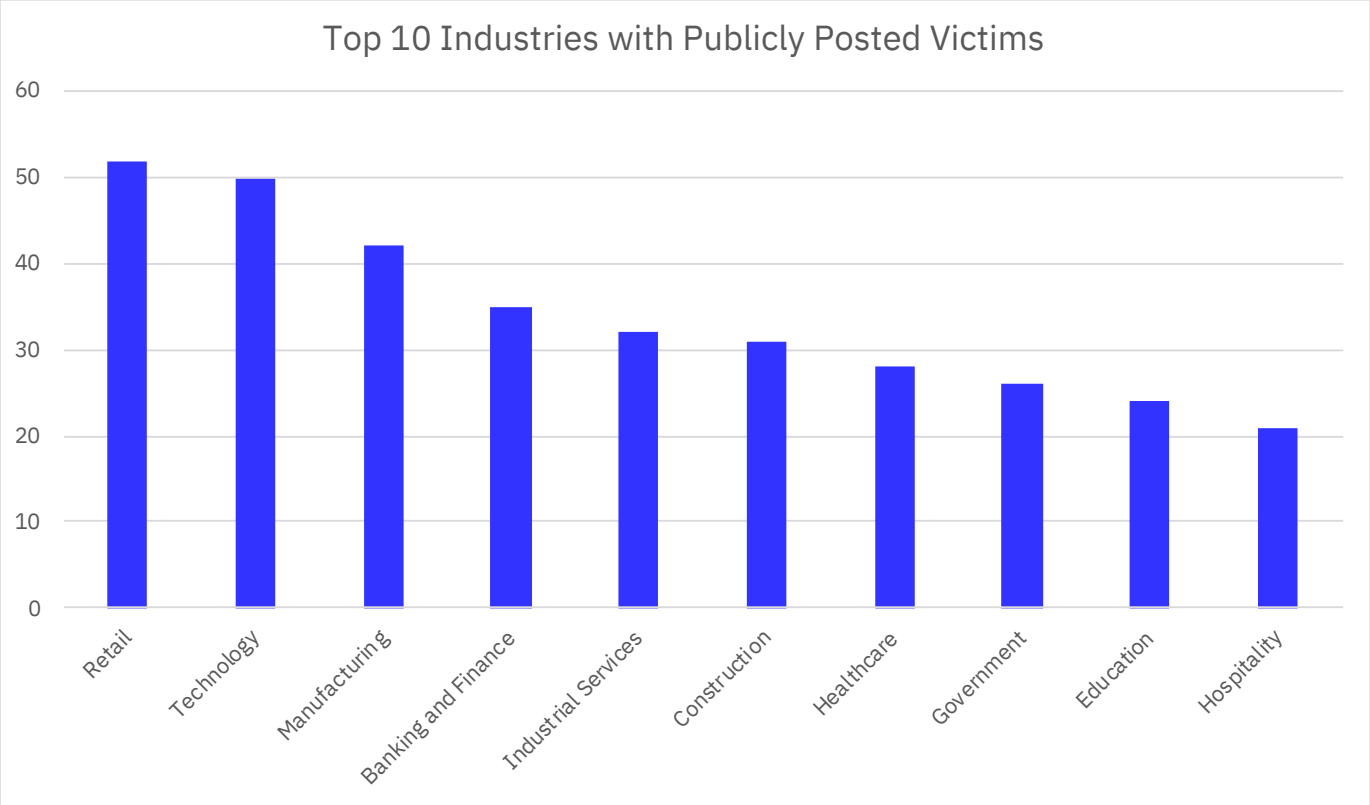

Figure 6: Top 10 Industries with Publicly Posted Victims

How Often are Victims Being Posted?

Publicly posting data exfiltrated from victim organizations remains a cornerstone of the double extortion methodology used by most ransomware groups to pressure victims into paying the ransom demand. The ransomware "industry" as a whole consistently adds new victims to their respective leak sites. As an "industry," the 40 ransomware groups we tracked publicly posted an average of 6.8 new victims every day in 2022. As of March 27, there were only five days in 2022 when there were no new additions to publicly posted ransomware victims across the tracked ransomware groups.

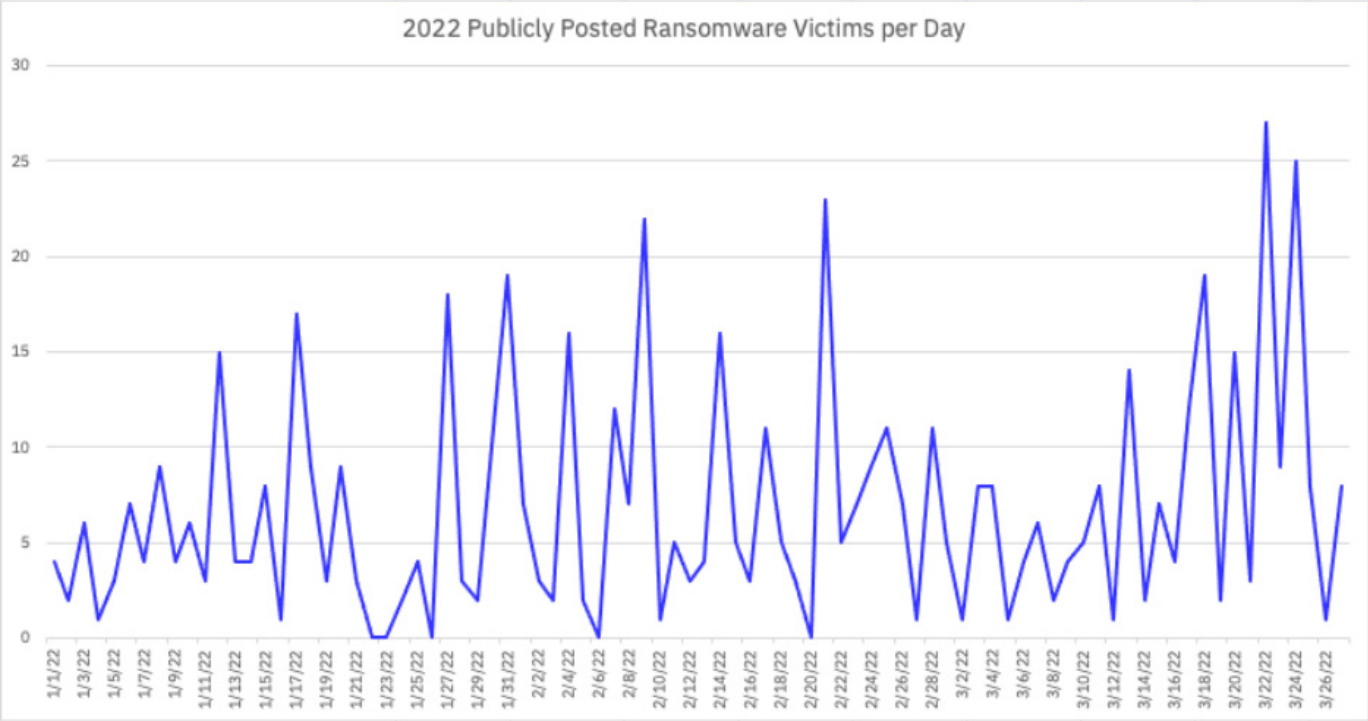

Figure 7: Publicly Posted Ransomware Victims per Day

During the same time period in 2021, the average number of public postings by ransomware groups was significantly lower at approximately four victims posted per day. When comparing the Q1 2021 and Q2 2022 data sets together, we see a pretty similar pattern, although lower in quantity.

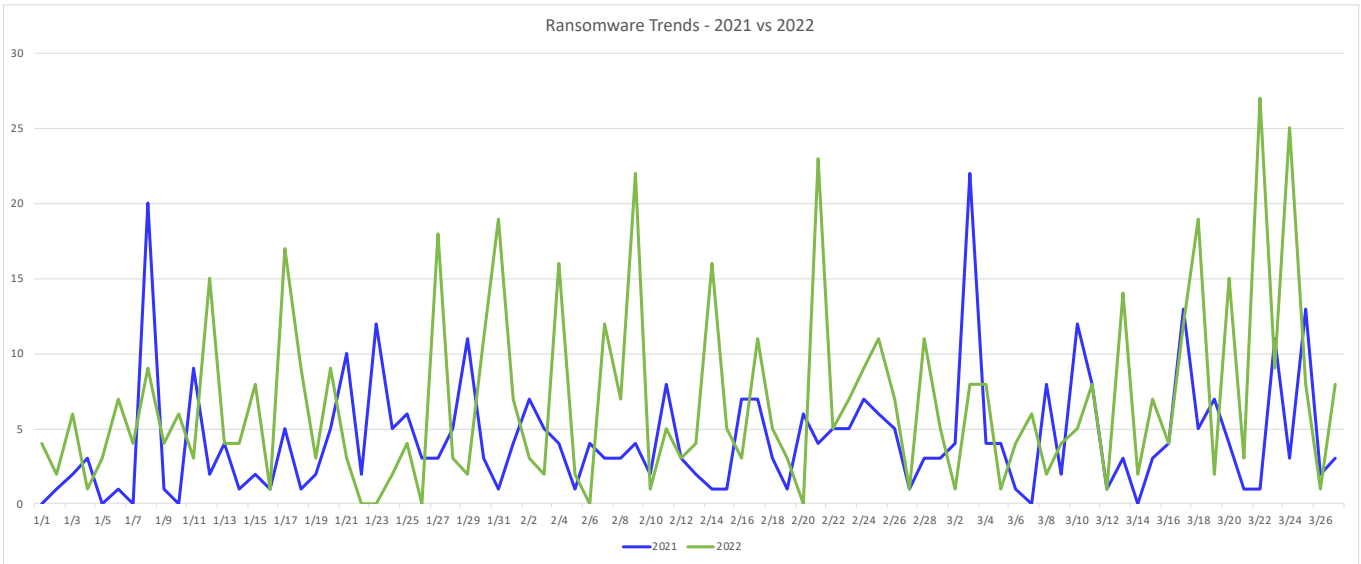

Figure 8: Ransomware Trends 2021 vs 2022 (Q1)

Based on the comparison between 2021 and 2022 ransomware trends, we are seeing the same types of peaks and valleys between the two data sets although 2022 has higher posting rates on average. Overall, 2022 is shaping up to be similar to 2021 on an amplified scale.

Ransomware Case Studies

The examination of initial ransomware trends in 2022 tells a very similar story to what we experienced with ransomware in prior years, yet there are some unique scenarios that are adding to the complexity of the ransomware landscape. We will examine two different case studies; the Ukraine/Russia conflict, and the 2022 Conti Ransomware Group Leaks. This will help us evaluate their potential impacts on ransomware trends in 2022.

Case Study One: 2022 Russian Invasion of Ukraine

The Russian invasion of Ukraine is shaping up to be one of the most significant events of 2022 (and we are only finishing Q1!). Throughout the events leading up to the invasion and beyond, there has been a strong cyber component of the Russian military strategy that has rarely been seen before. The kinetic and cyber components of the conflict have introduced a complexity in the threat landscape that many would argue should have some impact on how ransomware groups are able to operate.

Our hypothesis was that the Ukraine/Russia conflict would have an impact on ransomware operations, specifically that the conflict would slow them down.

Conti's Messaging Around the Ukraine/Russia Conflict

Two of the most prevalent ransomware groups in 2022, Conti and Lockbit, both had notable but opposing reactions to the Ukraine/Russia conflict. Let's start with Conti's messaging, which came in two separate updates on their leak site "Conti News." Their statements came across as aggressive with threats of attacking the critical infrastructure of "enemies", and gave a sense of internal struggle between the group's members. One statement declared support for Russia while the other was not explicitly supporting the Russian government, but rather was in support of defending Russian critical infrastructure and spoke maliciously of western countries.

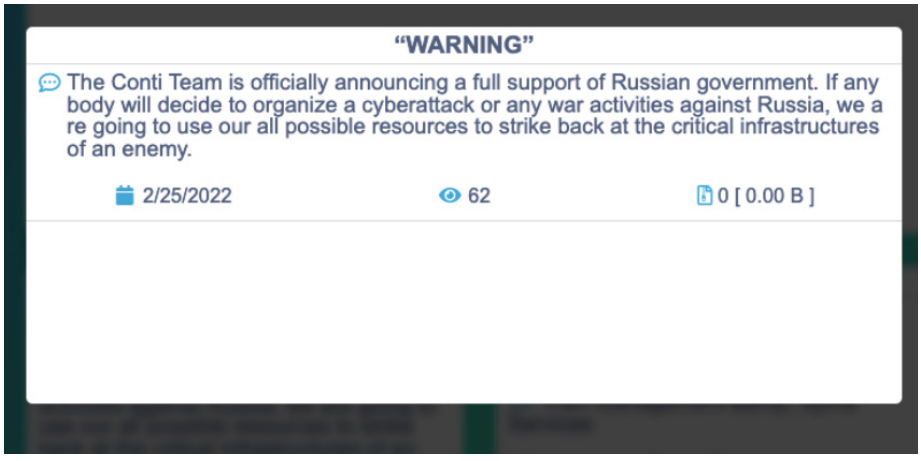

Figure 9: Conti's Original Reaction to the Russian Invasion of Ukraine

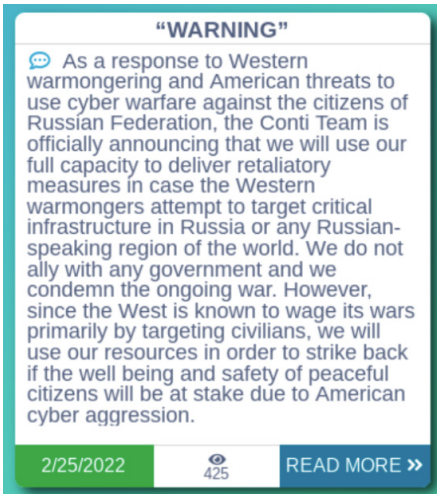

Figure 10: Conti's Follow-On Reaction to the Russian Invasion of Ukraine

Conti Ransomware Trends During the Ukraine/Russia Conflict

Conti had a relatively slow start to 2022 but had a large spike in public victim postings on January 7 when they published seven victims to their Conti News leak site. Leading up to the Russian invasion of Ukraine, Conti had relatively few public victim postings compared to other ransomware groups, including Lockbit.

Figure 11: Publicly Posted Conti Victims per Day

As Russia officially launched its invasion of Ukraine on February 24, 2022, Conti's public posting of ransomware victims began and continued to increase and remain steady through the end of Q1 2022. When comparing the same time period in 2021, we see a very similar trending pattern, but with a higher average rate in 2022. In 2021 we see a long period of inactivity from the group spanning almost 2 months compared to the week of inactivity in 2022.

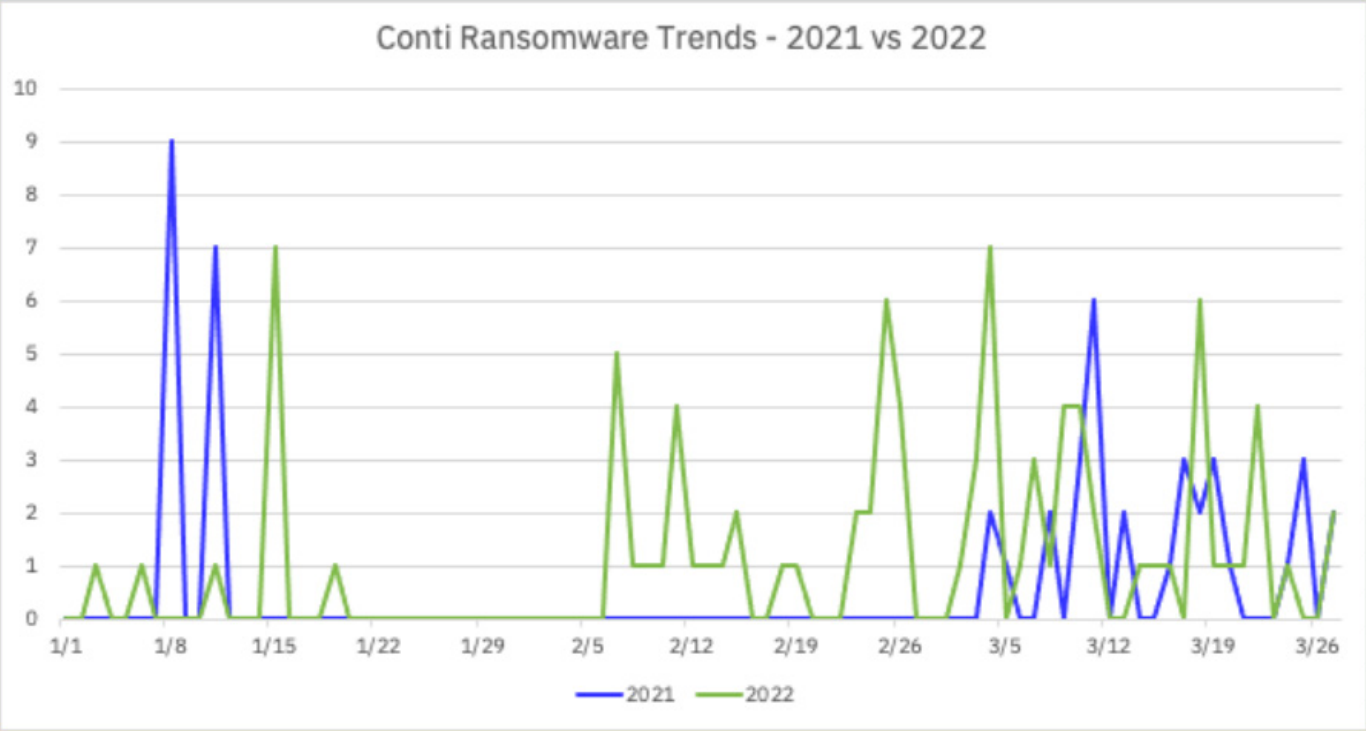

Figure 12: Conti Ransomware Trends - 2021 vs 2022

Examining dates closer to the Russian invasion of Ukraine, we see that compared to Conti's 2022 average rate of public victim postings, their activity leading up to the Russian invasion was slightly below their average posting rate while their public postings significantly rose after Russia began their invasion of Ukraine.

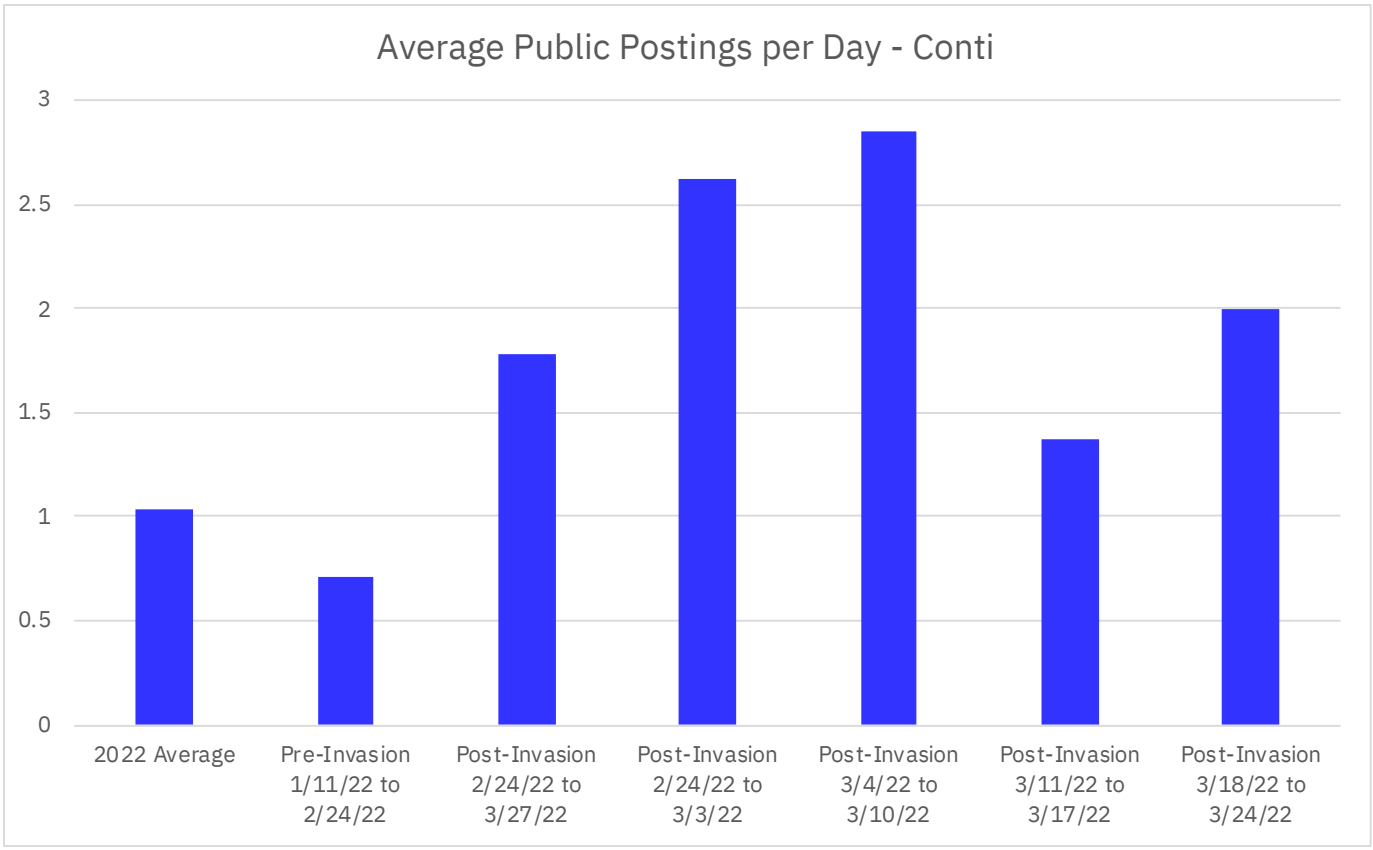

Figure 13: Conti's Average Public Postings per Day

Based on the available data regarding Conti's publicly posted ransomware victims, it appears that the Ukraine/Russia conflict did not cause a slow down in operations, rather, their operations increased during this time period.

Lockbit's Messaging Around the Ukraine/Russia Conflict

Lockbit's stance on the conflict was quite the opposite of Conti's messaging. Lockbit explicitly indicated that they would "never, under any circumstances, take part in cyber-attacks on critical infrastructures of any country in the world or engage in any international conflicts." Their message also focused on the fact that they view themselves as "post-paid penetration testers" and that, for them, "it is just business." As they issued this message, they also indicated that they would be publishing all available data from victim organizations in response to the Ukraine/Russia conflict.

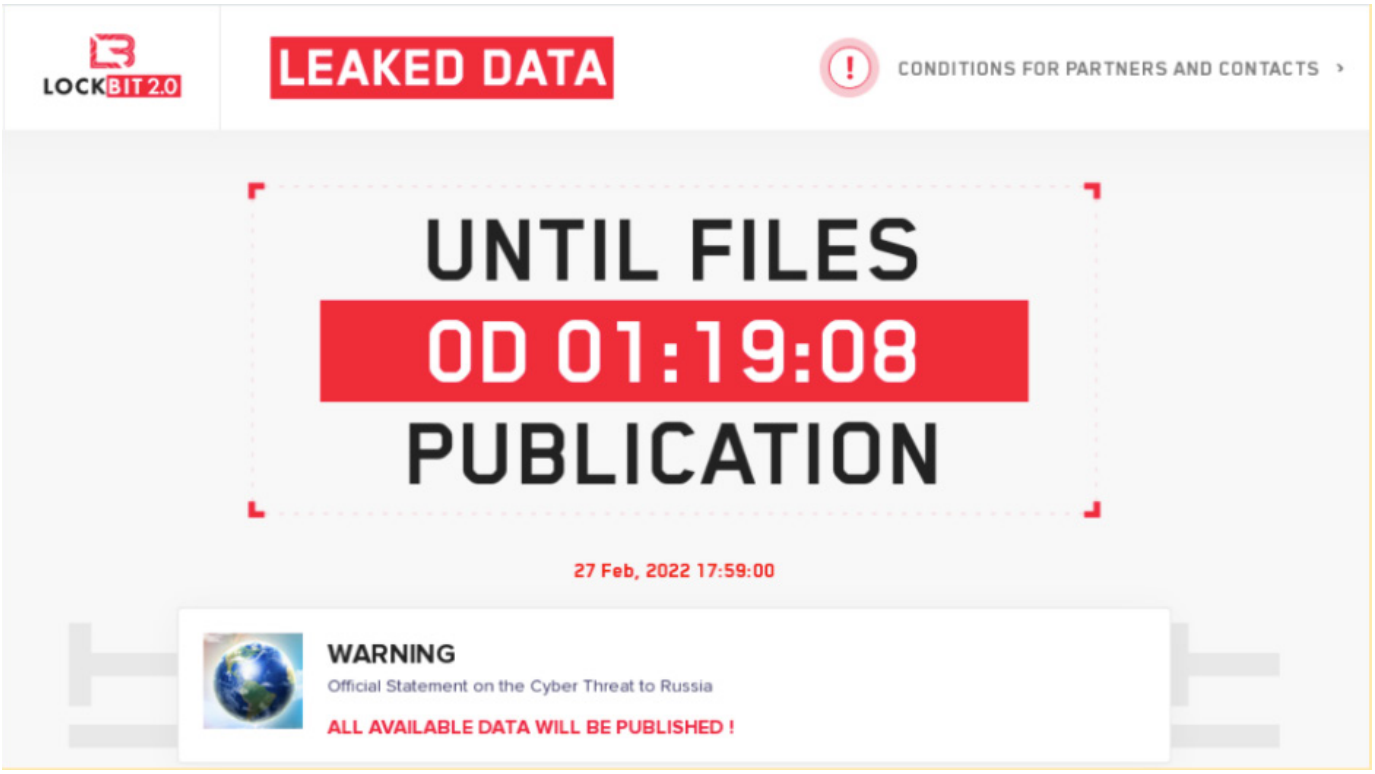

Figure 14: Lockbit's Response to the Ukraine/Russia Conflict

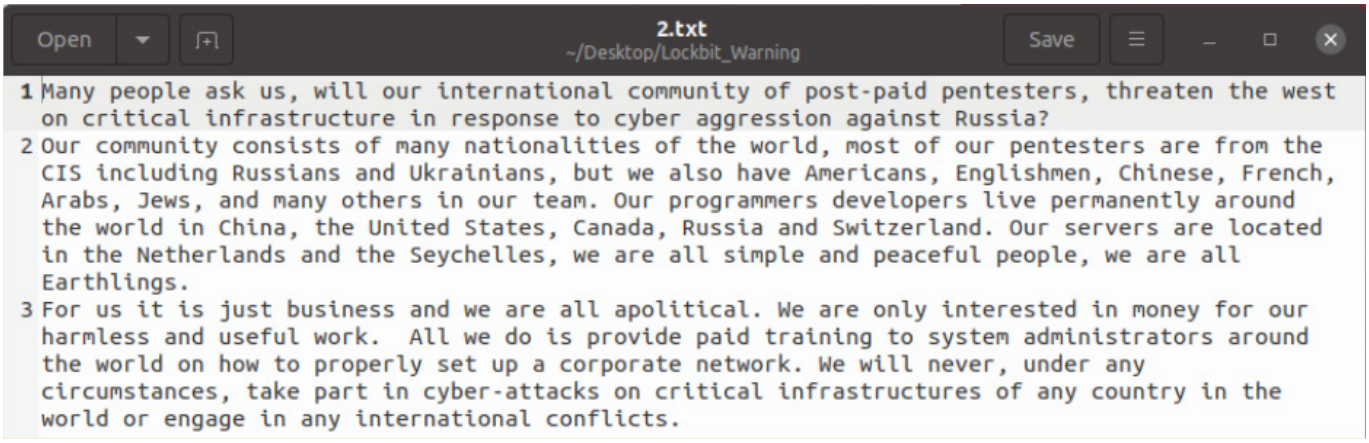

Figure 15: Further Details on Lockbit's Response to the Ukraine/Russia Conflict

Lockbit Trends During the Ukraine/Russia Conflict

Lockbit started 2022 with daily victim postings around or exceeding the 2022 average for all ransomware groups. Moving into late January and beyond, Lockbit operated significantly above their 2022 average until the third week of the Russian invasion in Ukraine when they had a short-term slowdown. Starting in the fourth week of the Russian invasion, Lockbit's daily victim posting significantly increased, exceeding the 2022 average rate for all ransomware groups' daily postings[3].

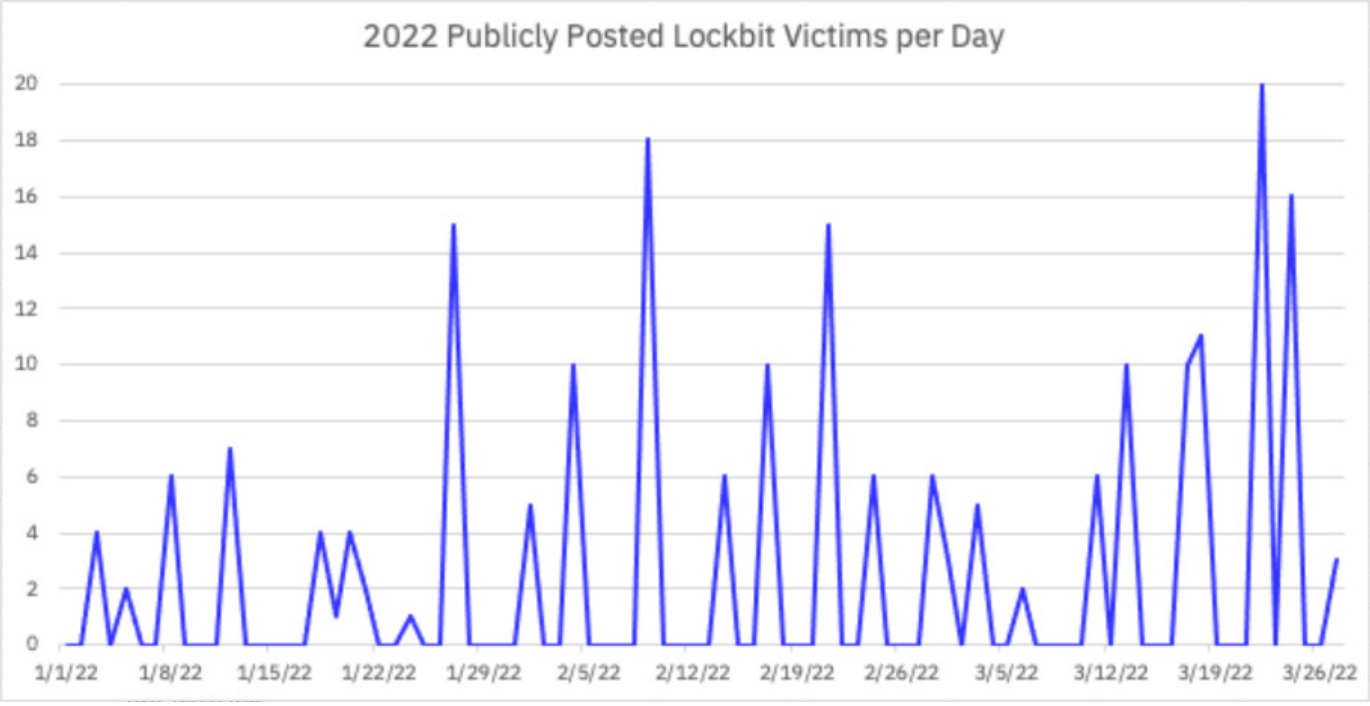

Figure 16: Publicly Posting Lockbit Victims per Day

Examining dates closer to the Russian invasion of Ukraine, we see that compared to Lockbit's 2022 average rate of public victim postings, their pre-invasion victim postings rate was below their 2022 average rate of victim posting. As the Russian invasion of Ukraine began, there was a slight uptick in victim postings with a significant one-week drop-off. Into the fourth week of the Russian invasion and beyond, Lockbit significantly increased their rate of public posting of ransomware victims.

[3]We were unable to perform analysis of Lockbit 2021 trends due to Lockbit 2.0 emerging late in 2021 with their leak site.

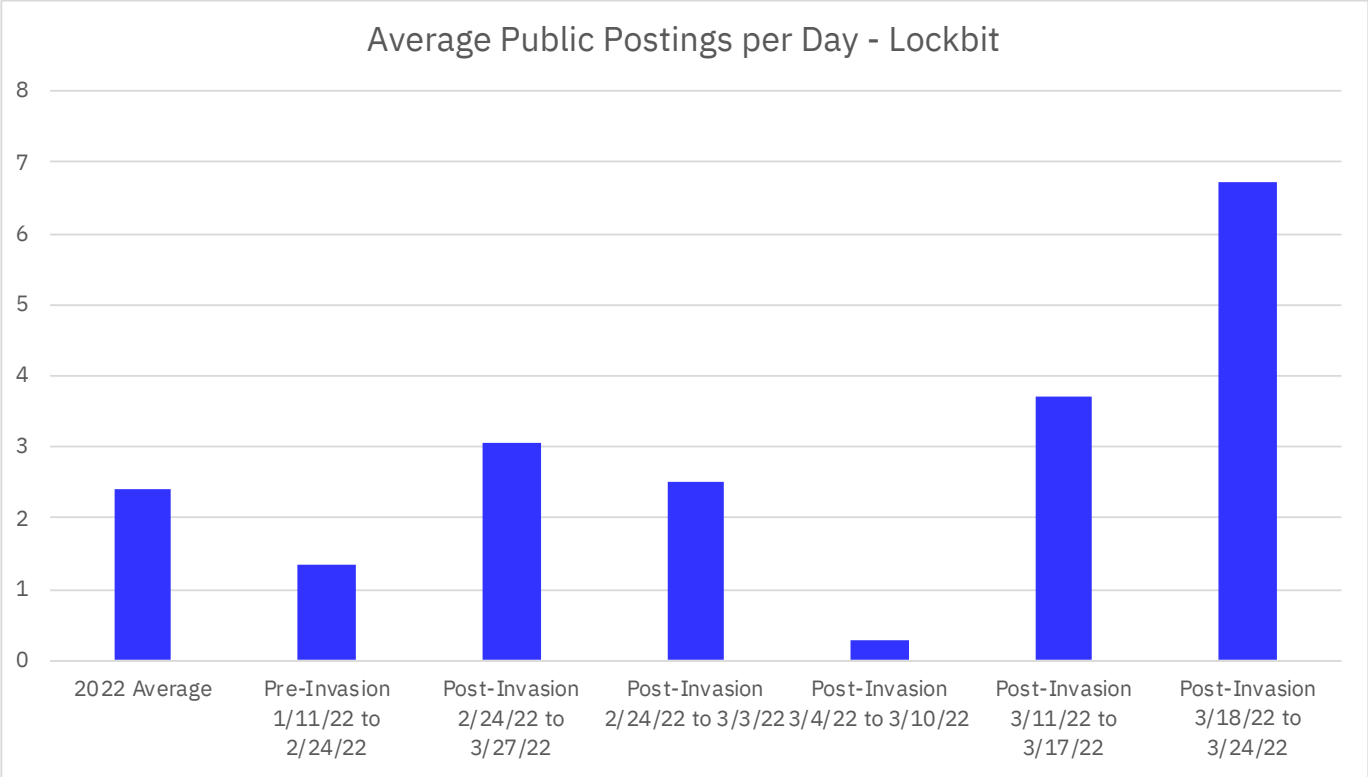

Figure 17: Lockbit's Average Postings per Day

Similar to our observations of Conti's activity, Lockbit's rate of publicly posted ransomware victims did not appear to be hindered by the Ukraine/Russia conflict, rather, with the exception of one week of reduced public victim postings, their operations increased during this time period.

Ukraine/Russia Case Study Conclusions

Our hypothesis was that because of the severity of the conflict and all of the complexities added by cyber and kinetic components of the conflict, ransomware operations would be hindered. However, our examination of Conti and Lockbit operations before and after the Russian invasion of Ukraine shows that the case may not be that simple. Conti's operational tempo in 2022 is quite similar to their operational tempo in 2021, and in fact, their tempo has increased as the invasion of Ukraine has progressed. Similarly, Lockbit started 2022 off with high rates of public victim postings, and with the exception of a few short stints, has remained at the front of the pack for total victim postings.

When looking at the larger data set of all ransomware groups, we see this trend hold firm. Leading up to the Russian invasion of Ukraine, ransomware operations remained at or above the 2022 average for victim postings per day, and with the exception of the second week of the Russian invasion, the number of ransomware public victim postings increased as the invasion continued.

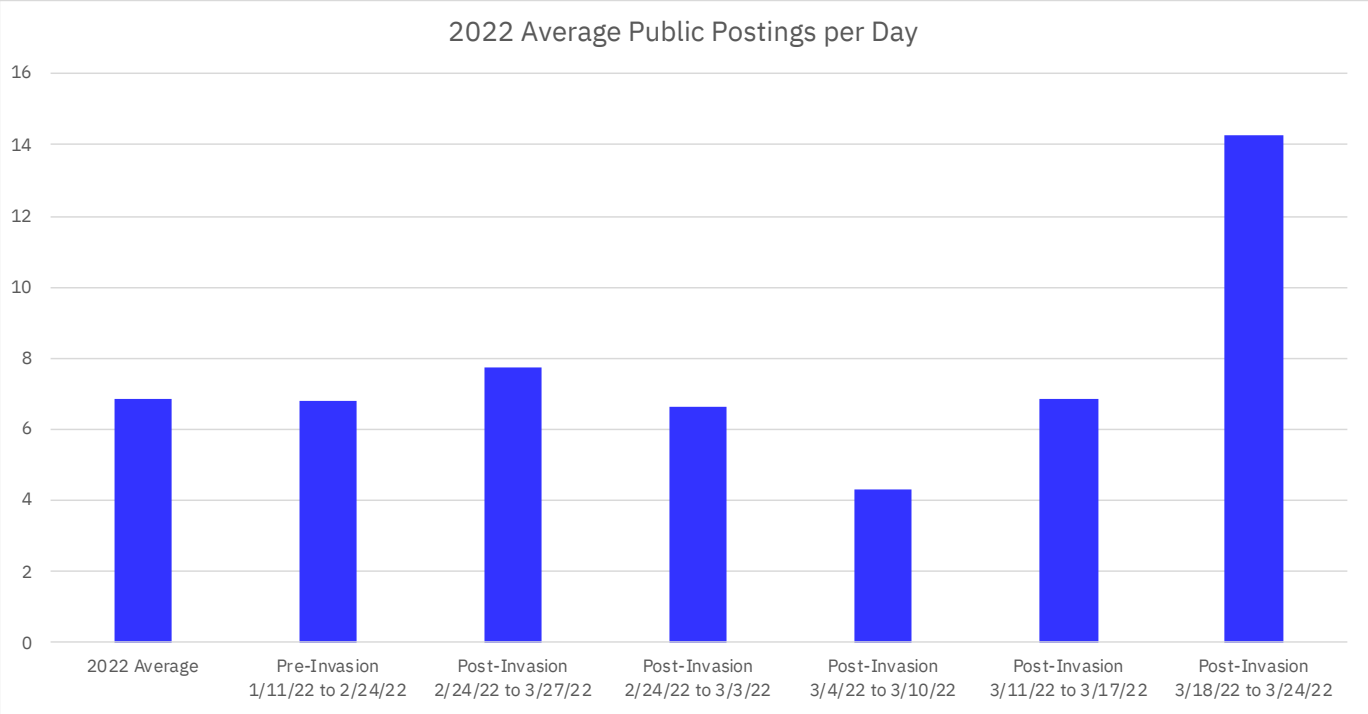

Figure 18: Average Public Victim Postings per Day

As discussed in the sections above, 2022 public victim postings are on the rise compared to 2021, providing further evidence that the Ukraine/Russia conflict may not have impacted ransomware operations as previously hypothesized.

Case Study Two: 2022 Conti Ransomware Leaks

On February 27, 2022, a Twitter account called @ContiLeaks began leaking information about the Conti ransomware group in support of Ukraine. Included in these leaks were chat logs of the Conti group's' developers and affiliates, source code for the Conti ransomware and decryptor, and other sensitive information about the Conti ransomware group's operations. With these leaks, security researchers were able to gain critical insight into how the Conti group operates, who the major players are, bitcoin wallets associated with their operations, and more. At first glance, this is the type of leak that you would expect to cripple a criminal enterprise like Conti's.

Examining Conti's public victim posts to their Conti News site since February 27 paints a slightly different picture. A few days after the initial Conti leaks occurred, public victim postings for Conti sharply increased and remained higher than their 2022 average posting per day rate through the end of our analysis period.

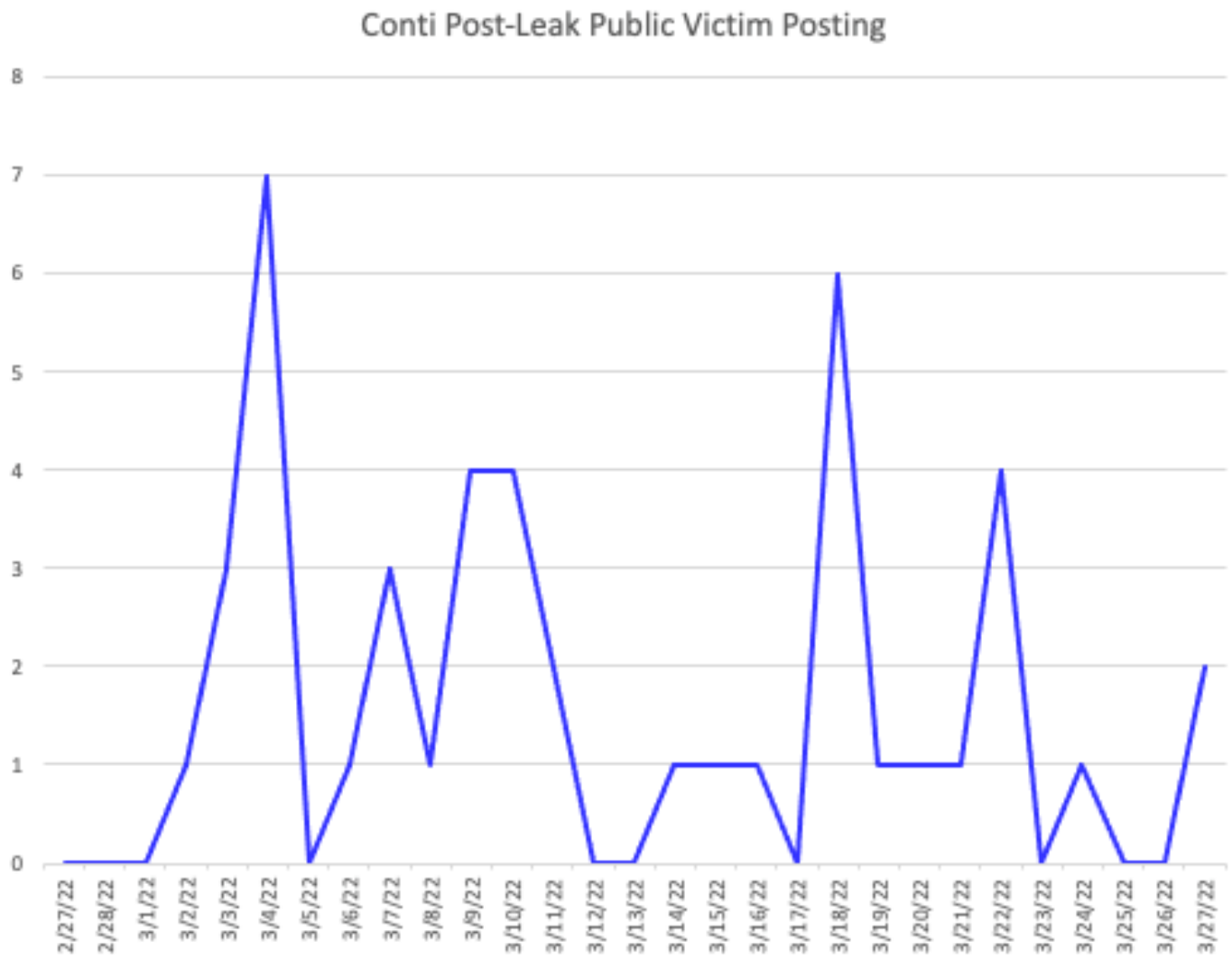

Figure 19: Post-Leak Conti Public Victim Posting

Conti Leaks Case Study Conclusions

Conti has gone through two major leaks in less than 12 months, the first in August 2021 when a Conti affiliate leaked many of their playbooks and non-ransomware utilities. Now, beginning in February 2022, they have had another leak that resulted in sensitive information and the source code to their ransomware. Nonetheless, Conti has been able to weather these leaks with seemingly no short-term impact to their ransomware operations. They are continuing to post newly compromised victims and continue operations as they have in years past.

More time and data will tell the long-term implications for the Conti ransomware group, but, for now, it's business as usual for them.

Overall Ransomware Conclusions

To those of us who are security practitioners, ransomware has been top of mind for many of the decisions that we make. In most cases, the encryption of files and exfiltration of sensitive data is the worst-case scenario, and if it happens, it's probably the worst day of our career. The fear of being successfully hit with Ransomware is always in the back of our minds.

For those of us taking a peek into the ransomware world for the first time, rapidly evolving scenarios like the Ukraine/Russia conflict, recent Lapsus$ activity, or the recent critical Chrome vulnerability, may give the impression that ransomware is trending downward, or that it's not the problem it used to be. However, as the data from 2022 is currently showing us, ransomware is still a huge threat for all organizations across all industry verticals.

Throughout our research we have come to the following key conclusions pertaining to ransomware operations and the influence of external sources:

1. Ransomware groups are resilient and can maintain operational tempo amidst significant international events and crises

Our original hypothesis was that ransomware groups operating out of eastern Europe and Russia would be impacted by the Ukraine/Russia conflict. After examining the data associated with 2022 publicly posted ransomware victims, that hypothesis was not proven to be true. When comparing 2021 to 2022 ransomware data, we see a higher average rate of public victim postings across all ransomware groups. It is important to note that there was a slight downtrend in all ransomware groups starting in late February 2022 and lasting until late March 2022. It is possible that there was some impact from the Ukraine/Russia conflict, but this downtrend also looks similar to the same time periods in 2021, which may indicate other conclusions to be drawn from the slowdown.

Looking at Conti and Lockbit specifically, we see that average public postings during the Ukraine/Russia conflict either remained close to their 2022 averages or went up. Lockbit showed a one-week drop off in activity during the Ukraine/Russia conflict, however, that pattern of activity is also not uncommon in their 2021 trends.

Looking to the future, longer-term tracking and analysis of international events and their impact on ransomware operational tempo will help us determine what types of events have the most impact on ransomware groups. Additionally, it would be beneficial to conduct supplemental research to factor in additional external variables such as cyber insurance, victim willingness to pay ransoms, and economic sanctions, both of which can have an impact on ransomware group public posting rates.

2. Ransomware groups can undergo significant information leaks with minimal short-term impacts on their operations

Conti has had two significant data leaks over the past 12 months. Our original hypothesis was that a ransomware group would not be able to sustain operations after a leak of this magnitude. Based on our review of short-term data associated with Conti's operations, we have not proven this hypothesis to be true. Conti has continued to operate and publicly post ransomware victims to their Conti News site. Overall, Conti operations have not been significantly affected by this leak, yet.

We will continue to track this hypothesis from a long-term perspective to determine if the data shows a slowdown in their capabilities. It is also possible that international events are having an impact on law enforcement's ability to take action, or perhaps that is in motion but not being executed yet. More time and data will show whether this hypothesis can be proven, or if they continue to operate as they do now.

3. Ransomware continues to trend upward

For security practitioners that are battling ransomware regularly, this conclusion isn't surprising in the least. But for individuals that are not dealing with ransomware on a regular basis, this might be a bit of a revelation. We are regularly alerted to new critical vulnerabilities, new exploitations, and new malware, and while new ransomware is certainly sprinkled into those alerts, it still doesn't get as much attention as it should. Since 2018, ransomware has been a significant threat that has evolved and grown more dangerous for organizations across all verticals. Looking at the 2021 and 2022 data, we are seeing 2022 start off at a faster rate than last year. With more than 40 ransomware groups regularly operating and posting public victims to their leak sites, it can be hard to keep up with how frequently this activity occurs.

Bottom Line, ransomware is still a very real problem.

Future Research

During our research into 2022 ransomware trends and the impacts of external events, we identified several additional research areas that we intend to investigate the following areas:

- Long-term, deep-dive analysis of ransomware groups including Conti, Lockbit, and others to identify trends in their operations including most commonly targeted countries, industries, and overall historical activity.
- A comprehensive 2022 review of ransomware trends and a re-evaluation of our hypotheses from this research.

And Finally... Why Threat Intelligence Matters

If the Ukraine/Russia conflict and the 2022 Conti leaks have confirmed anything for our industry, it is that events and intelligence from the cyber world happen fast. In fact, it happens really fast and it can be extremely difficult to keep up with all of the various information sources, blogs, Twitter threads, informal conversations, Slack channels, and whatever other sources you are focusing on for staying up to date. Understandably, keeping up to date with threat intelligence in itself is hard, but having contextual threat intelligence that is operationalized in your environment can be even harder.

What is Threat Intelligence Anyway?

If a tree falls and no one is around to hear it, does it make a noise? We think it does. Similarly, if a threat intelligence headline is read in a Slack channel and then never acted upon, is it threat intelligence? This is where the conversation starts to get interesting.

Oxford's definition of intelligence includes, "the ability to acquire and apply knowledge and skills." In our opinion, this holds true for threat intelligence as well. So going back to our original question, if blogs, threat feeds, data, or anything else relevant to the threat landscape is dropped in a slack channel, or shared and discussed, but then never acted upon or applied to your cybersecurity apparatus, is it threat intelligence? We would argue no, but it has the opportunity to be. It is not truly intelligence until it has been contextualized and operationalized in your environment. Until then, it's more of a data source than it is threat intelligence.

Operationalizing Threat Intelligence

The name of the game is taking all this data (from our seemingly endless supply of sources) and focusing on the consolidation, contextualization, and integration into our operational cybersecurity groups including SOC, vulnerability management, and IT. This can be a daunting task, but it doesn't have to be. Using a controlled approach, your organization can benefit from having operationalized threat intelligence to keep your security program up to date and as effective as possible.

Have a Platform That You Can Control

With so many data sources, it is extremely important that the organization have a place to consolidate, deduplicate, and store all of this data so that it can truly become threat intelligence. Most often, this is going to require a Threat Intelligence Platform (TIP).

Regardless of the TIP that you choose, it is important to be able to control and administer the platform. This is a key component of being able to operationalize threat intelligence in your environment. Without the ability to control and manipulate your TIP, you lose flexibility in designing, scaling, and augmenting your processes to make them as efficient as possible. You want the TIP to flex and support your workflows, and not the other way around.

Most TIPs on the market today give you the base functionality of storing and deduplicating data as it is ingested into the platform. Choosing a TIP that also has the ability to enrich intelligence through multiple sources is a huge win for contextualizing threat intelligence for your organization. TIPs that allow you to choose the best enrichment sources for your organization are extremely important for keeping the context relevant to your organization and industry vertical.

Automate and Orchestrate Where Possible

Cybersecurity and IT practitioners both have a love for automation and orchestration. Automation and orchestration is a force multiplier and allows us to accomplish more with our time. It even allows us to not have to do some of those mundane tasks that we all "love" to do. Another reason to love automation and orchestration is because it helps us operationalize the threat intelligence that is being ingested into our TIP.

As the confidence level of our vetted intelligence increases, it becomes more likely that we are going to take action and block IOCs, hunt for behaviors, or some combination of the two. With automation and orchestration capabilities included, or supplemented, with your TIP, you are now able to decrease the amount of time it takes to get detections in place. This means that we are more likely to be able to keep up with how fast the cyber world moves which is a big win for our proactive defense capabilities.

There are a lot of positives that come along with automation and orchestration, but there is a proper way to ensure organizations mature into automation. As the old adage goes, “Crawl, Walk, Run” describes how organizations need to fine-tune their processes well before considering automation and orchestration even with the temptation of “turn-key” solutions. Blocking unvetted or low confidence IOCs can have unintended consequences that may lead to the cybersecurity organization losing confidence in your threat intelligence program. Vetting and curating threat intelligence is a critical component of ensuring automation and orchestration are successful in adding to your defense posture and not taking away from it.

View Your Attack Surface from the Attacker’s Perspective

We often think of our attack surface as it relates to where our firewalls sit, or how many vulnerabilities our internal servers have, but in reality, if we think of our attack surface from the attacker’s perspective, we see that our attack surface consists of so much more than we originally thought.

As technology–specifically cloud-based technologies–has become an integral component of most organizations, our attack surface deviated from the traditional firewall-based perimeter that we were used to and dramatically increased the environments we needed to defend. This is why viewing your attack surface from the attacker’s perspective is extremely valuable to operationalizing threat intelligence.

As we mentioned above, threat intelligence is most impactful when it is contextualized. In order to contextualize our threat intelligence, we need to know what we have visible to attackers. If we implement methods of discovering new assets, especially those related to shadow IT, and discover details about critical services running on those assets, we are now placing ourselves in a proactive posture to be able to operationalize contextual threat intelligence for those assets. The end result is improved defenses of assets and a reduction of intrusion vectors for attackers.

Have Eyes and Ears on the Dark Web

Most organizations become the victim of an attack, whether it is phishing-related or there was a vulnerability on a server that was exploited. Perhaps there is an open RDP server on the internet that hasn’t been discovered internally yet. In many cases, threat actors often discuss these events on dark web forums and marketplaces before they become a high risk for the impacted organizations.

Having threat intelligence related to dark web forums and marketplaces is a great data source for being able to quickly and efficiently discover compromised credentials, newly vulnerable assets, or other threat actor discussions that specifically reference your organization. Having a pulse on what the threat actors are discussing is a great way to reduce the time to discovery of potential incidents and for closing gaps in your security posture.

This is Why Threat Intelligence Matters

Threat intelligence matters because cybersecurity moves fast. As the Ukraine/Russia conflict showed us, the amount of intelligence that was produced in an extremely short period of time can be overwhelming. We need methods of contextualizing and operationalizing threat intelligence quickly and efficiently.

Having a threat intelligence platform you can control and modify to suit your workflows and implementing automation and orchestration into your processes reduce the time to contextualize and operationalize threat intelligence in your organization. Monitoring your attack surface from the attacker's perspective and keeping a pulse on the dark web incorporate the attacker mentality into your threat intelligence strategy, further improving your cybersecurity capabilities. All of these powers combined (Captain Planet anyone?) yield an improved threat intelligence capability that keeps you up to date with current events and trends, scales your ability to use operationalized threat intelligence effectively, and aims to put you on even footing with the threat actor, for once.

GUIDEPOINT SECURITY

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132