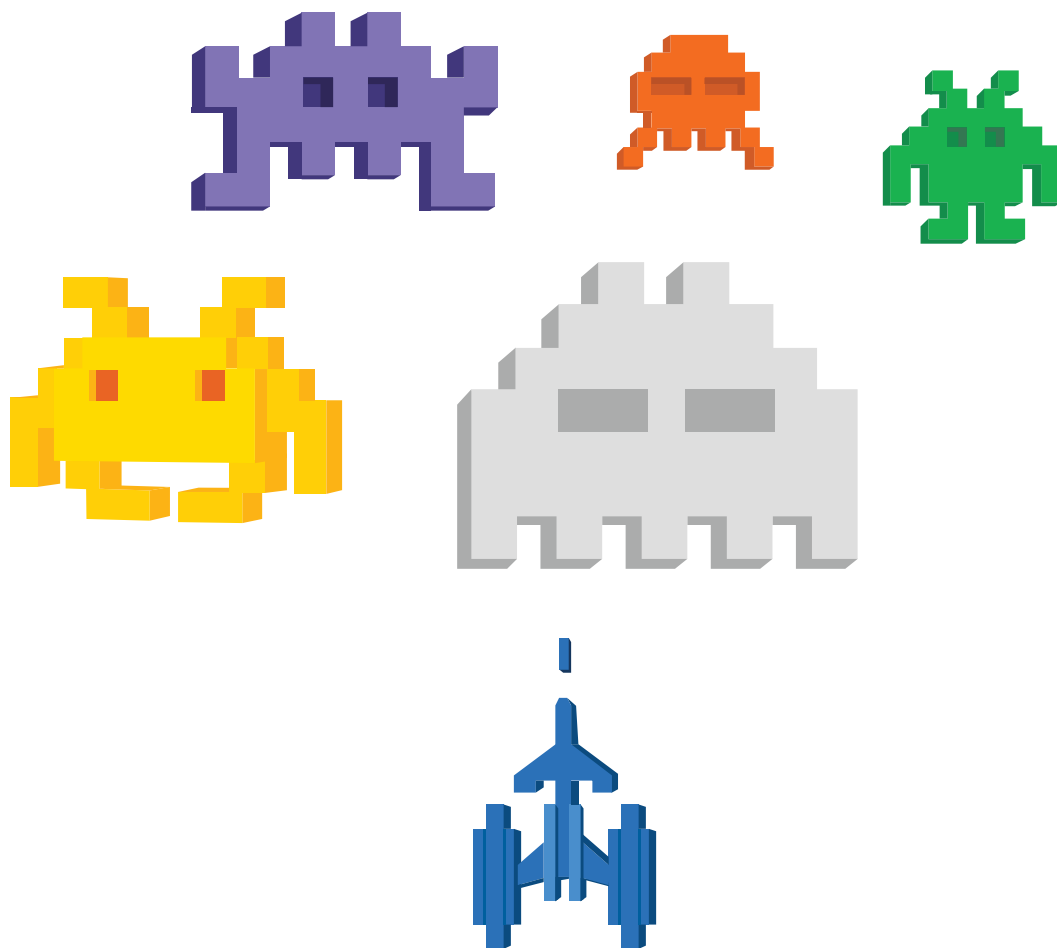


5 Ransomware Trends to Watch in 2020

By Allan Liska



This is the fourth year that Recorded Future has asked me to write up my [predictions](#) for where ransomware is headed in the coming year. Trying to predict the future when it comes to these attacks is always a challenge. Unfortunately, the one prediction that I am confident in is that ransomware attacks will continue to grow as cybercriminals get more sophisticated in their methods and expand their reach. In fact, two verticals that we are following closely — [state and local governments, and healthcare](#) — have both seen a 20% increase in ransomware attacks over this time last year (with the caveat that the numbers are small this early in the year).

There were two big ransomware stories in 2019. The first was that almost every industry was hit hard. [Local governments, healthcare, manufacturing](#), and even [finance](#) — there was no industry that was safe from increasingly sophisticated ransomware attackers. The second big story is that ransomware cybercriminals are threatening to [release files](#) when victims refuse to pay the ransom, and they're often following through with it. This means that even if organizations do everything correctly in their response to a ransomware attack, they could still be on the hook to pay the attacker hundreds of thousands of dollars or risk their sensitive data being leaked (or pay hundreds of thousands of dollars and still have their sensitive data leaked).

2020 is going to be a rough year. In my judgment, there are five major trends to watch out for in 2020:

- 1. Courts will play a greater role in driving behavior of victims and criminals** — As the price of ransom keeps going up, there will be more incentive for victims to use the courts in novel ways to recover funds or stop ransomware actors from publishing information.
- 2. The “ransomware as a service” market will continue to flourish** — Ransomware as a service (RaaS) continues to be the best way for inexperienced cybercriminals to get started in ransomware, and underground forums are flooded with ads for different RaaS offerings at all price points.

- 3. There will be a continued separation between the ransomware “haves” and “have-nots”** — Despite all the headlines, pulling off a successful ransomware campaign is surprisingly difficult, and only a small proportion of threat actors will be successful. Many vendors on the criminal underground will scam more inexperienced criminals with inferior products.
- 4. The United States will lose victim market share** — While the United States accounted for 53% of all attacks between Q2 2018 and Q2 2019, and American victims will continue to make up the greater part of victims of ransomware attacks in 2020, ransomware actors are starting to focus their attention on other countries.
- 5. Publication of victim files will become more popular** — Already, many cybercriminals have either threatened to release the files of victims who refuse to pay or have done so. On the surface, this makes sense as a tactic: if the victims won't pay the ransom, the attacker may be able to extort victims in other ways. But it remains to be seen whether this will be a successful extortion strategy for the ransomware actors.

Let's look at each of these trends in greater depth.

1. We Expect the Courts to Play a Greater Role in Driving Behavior of Victims and Criminals

As much as we would all like to be able to drag the cybercriminals behind ransomware to court, it is doubtful that we will see much of that. Victims and their insurance companies, however, are getting smarter about ways to use the legal system to fight back.

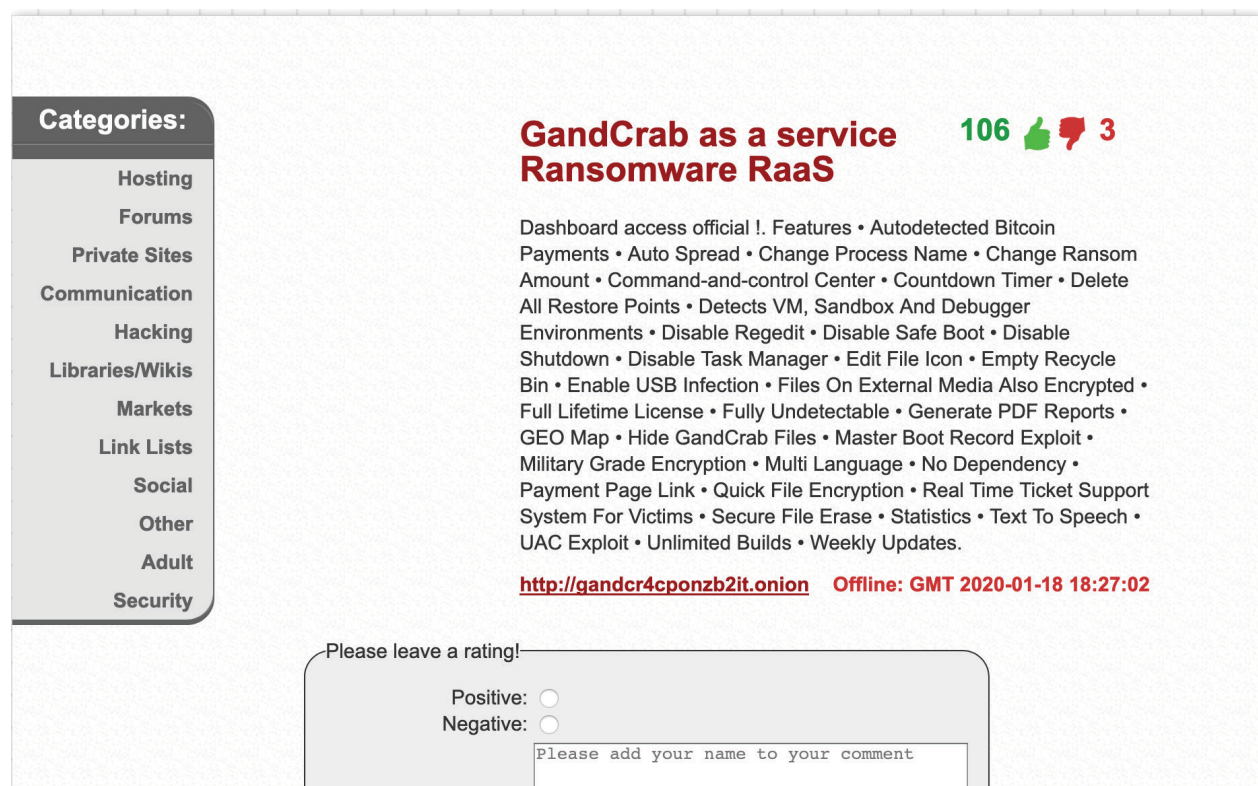
When the team behind the MAZE ransomware published stolen data from Southwire on a public-facing website, Southwire took them to court and got the [entire hosting company shut down](#). Threatening to release victim data only works when it is easily reachable. If the ransomware actors host stolen data on a public hosting company's servers, it opens up that hosting company to lawsuits. This won't end well for the hosting company, which will have to spend millions of dollars to legally defend itself, or for the ransomware actors, who will find it more difficult to locate resources to host their stolen content.

Ransomware relies on cryptocurrency, in part, because it is largely seen as “untraceable.” Bitcoin, specifically, is most often associated with ransomware because it facilitates quick payments, is easily exchangeable, and [most victims are familiar with it](#). As the law has started catching up to cryptocurrency technology, some of the perceived advantages of cryptocurrency are fading. For example, a British court ordered the exchange they used to [freeze the Bitcoin and release the customer](#) (the ransomware actor) information to the court.

Because the price of ransom keeps going up, there will be more incentive for victims to use the courts in novel ways to recover funds or stop ransomware actors from publishing information.

2. The RaaS Market Will Continue to Flourish

Ransomware as a service (RaaS) continues to be the best way for inexperienced cybercriminals to get started in ransomware, and underground forums are flooded with ads for different RaaS offerings. For anywhere from \$10 to \$3,000, an attacker can get started in the ransomware game, as shown in the image below).

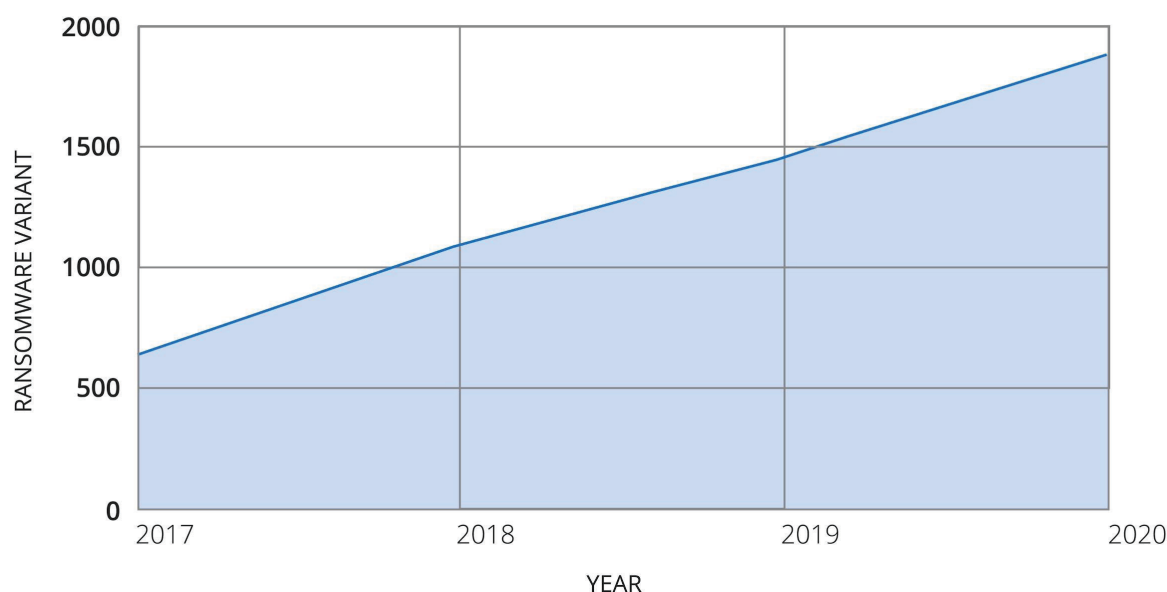


The screenshot shows a forum post for "GandCrab as a service Ransomware RaaS". On the left is a sidebar with categories: Hosting, Forums, Private Sites, Communication, Hacking, Libraries/Wikis, Markets, Link Lists, Social, Other, Adult, and Security. The main post has a title "GandCrab as a service Ransomware RaaS" with 106 likes and 3 dislikes. The post content lists various features: Dashboard access official!, Features • Autodetected Bitcoin Payments • Auto Spread • Change Process Name • Change Ransom Amount • Command-and-control Center • Countdown Timer • Delete All Restore Points • Detects VM, Sandbox And Debugger Environments • Disable Regedit • Disable Safe Boot • Disable Shutdown • Disable Task Manager • Edit File Icon • Empty Recycle Bin • Enable USB Infection • Files On External Media Also Encrypted • Full Lifetime License • Fully Undetectable • Generate PDF Reports • GEO Map • Hide GandCrab Files • Master Boot Record Exploit • Military Grade Encryption • Multi Language • No Dependency • Payment Page Link • Quick File Encryption • Real Time Ticket Support System For Victims • Secure File Erase • Statistics • Text To Speech • UAC Exploit • Unlimited Builds • Weekly Updates. Below the features is a URL: <http://gandcr4cponzb2it.onion> and a status: Offline: GMT 2020-01-18 18:27:02. At the bottom of the post is a rating section with "Positive:" and "Negative:" radio buttons, and a text input field with the placeholder "Please add your name to your comment".

A RaaS ad for GandCrab from early 2019.

I write this report the same time every year, so at the end of January, I always look at how many different ransomware variants Recorded Future is monitoring. For January 2020, that number is 1,886 (though, in reality, there are about 43 variants that account for the majority of attacks) — but let's take a look how the number has grown in the following figure:

Ransomware Variant Coverage by Year



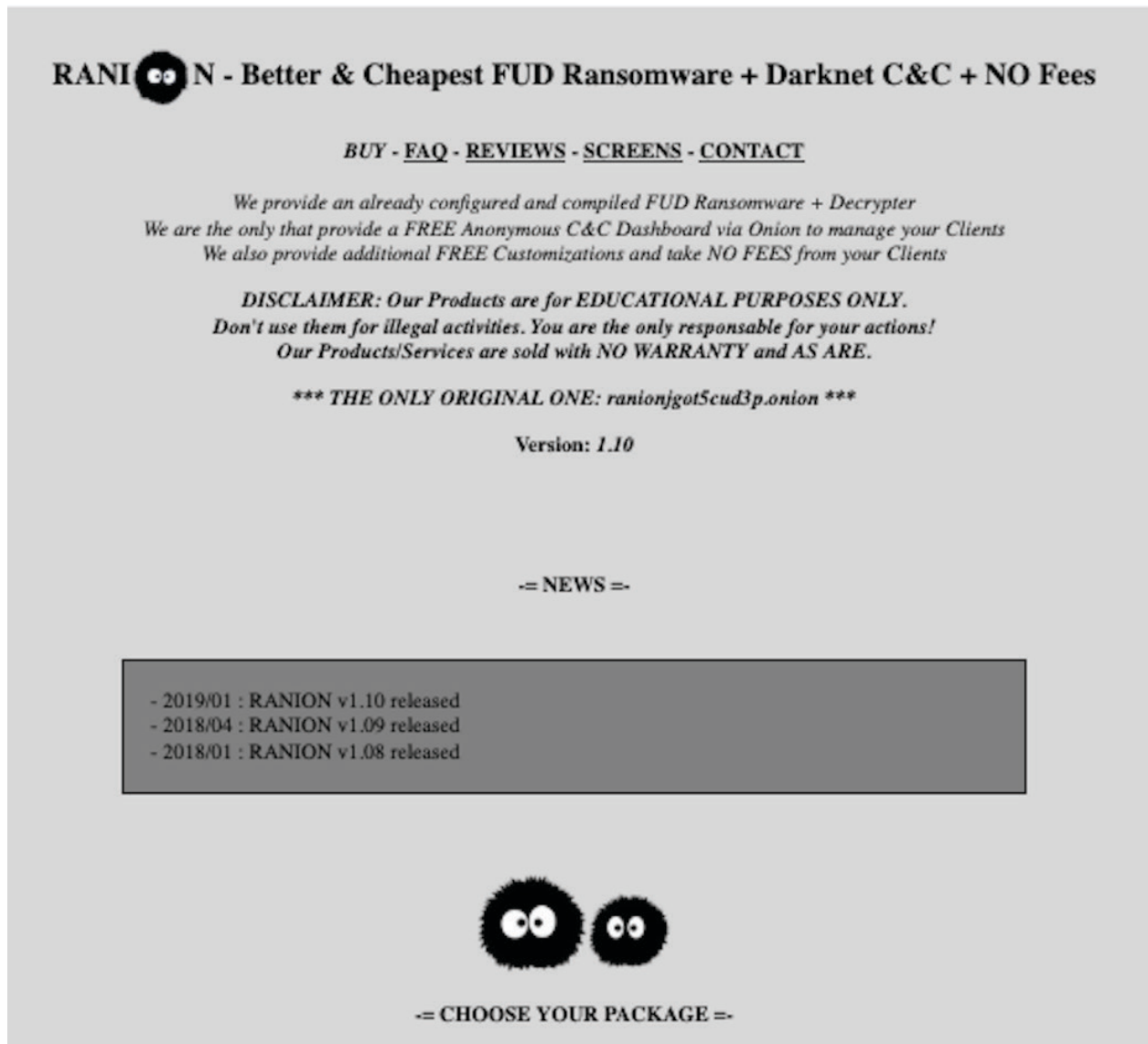
Recorded Future ransomware coverage by year.

Growth in the number of variants has been fairly steady over the years and it will continue to grow in 2020. There is a big demand for RaaS offerings in the underground market, and lots of people are willing to take the money of inexperienced wannabe hackers that don't know any better. This means we will continue to see plenty of offerings of ransomware as a service on the criminal underground in 2020.

3. Separation of the Ransomware 'Haves' and 'Have-Nots'

Despite all of the headlines, carrying out a successful ransomware campaign is surprisingly difficult. It takes planning and operational skill, and the attacker has to understand the victim's network and their business. There are some ransomware attackers who are very good at this — and they make a lot of money.

Most are not. Just as with other multi-level marketing schemes, RaaS leaves a few people with a lot of money, but most don't make any, and sometimes they even lose money. Take the ad in the image below for Ranion ransomware:



RANION - Better & Cheapest FUD Ransomware + Darknet C&C + NO Fees

BUY - FAQ - REVIEWS - SCREENS - CONTACT

*We provide an already configured and compiled FUD Ransomware + Decrypter
We are the only that provide a FREE Anonymous C&C Dashboard via Onion to manage your Clients
We also provide additional FREE Customizations and take NO FEES from your Clients*


**DISCLAIMER: Our Products are for EDUCATIONAL PURPOSES ONLY.
Don't use them for illegal activities. You are the only responsible for your actions!
Our Products/Services are sold with NO WARRANTY and AS ARE.**

***** THE ONLY ORIGINAL ONE: ranionjgot5cud3p.onion *****

Version: 1.10

== NEWS ==

- 2019/01 : RANION v1.10 released
- 2018/04 : RANION v1.09 released
- 2018/01 : RANION v1.08 released



== CHOOSE YOUR PACKAGE ==

Ad for Ranion ransomware.

The author behind this ransomware has been running this ad since 2017. Ranion has never broken the top 10 of any ransomware lists and has never been part of a significant breach. The only place anyone ever sees the Ranion ransomware is on VirusTotal reports because it has been flagged by someone's antivirus program, or because a researcher uploaded a new version. Despite that, people keep giving the author money to sign up for his service.

There are many scam artists on these forums looking to take advantage of suckers and sell them inferior products. The problem is, even bad ransomware actors get lucky sometimes, and this has been the case in many of the early attacks against state and local governments, where the ransomware attackers were able to capitalize on some of the security missteps of the teams responsible for protecting the town or city. It's important to stay vigilant and protect against these attacks.

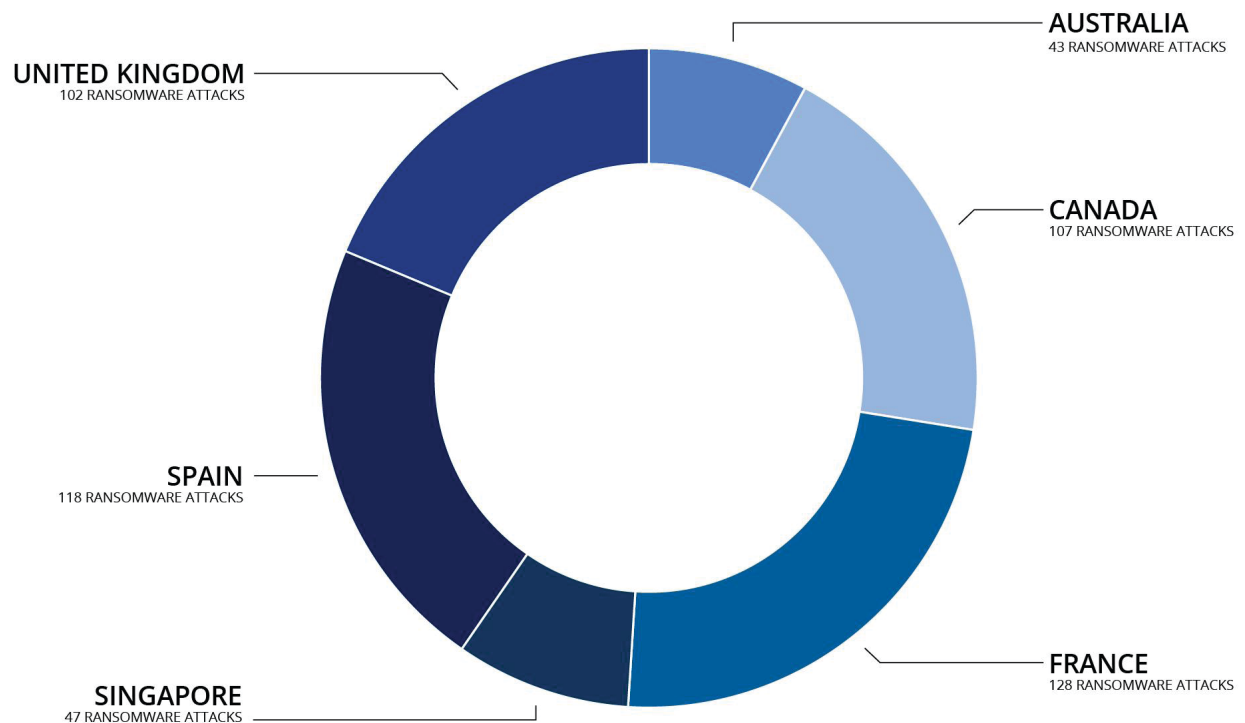
4. The United States Will Lose Victim Market Share

According to [Malwarebytes](#), the United States accounted for 53% of all attacks between Q2 2018 and Q2 2019, with Canada and the United Kingdom coming in a distant second and third, respectively. While the United States will continue to lead the world in ransomware attacks for the foreseeable future, ransomware actors are starting to focus their [attention](#) on other [countries](#).

The problem is, it's hard to quantify what that rise looks like. Most countries don't have reporting requirements for ransomware attacks, and press coverage of these attacks in most countries is sporadic at best.

Using open source reporting available in the Recorded Future platform, I tried to gauge the extent of ransomware attacks in Australia, Canada, France, Singapore, Spain, and the United Kingdom for 2019 to see what we could learn.

Number of Reported Attacks in 2019 by Country



The number of reported attacks by country.

As with all of our open source reporting on ransomware attacks, the real number is undoubtedly significantly higher, as the majority of attacks go unreported. The breakdown by sector varied by country, though again, this is only a fraction of all ransomware attacks in each country, so it might not be representative of the overall ransomware attack picture.

Australia	Canada	France	Singapore	Spain	United Kingdom
Utilities	Publishing	Publishing	Hospitality	Telecom	Finance
Publishing	Construction	Service	Banking	Service	Healthcare
Finance	Banking	Pharmaceuticals	Publishing	Petroleum	Pharmaceuticals
Automotive	Education	Metals/Mining	Education	Finance	Transportation

The top four sectors hit by ransomware attacks for each country.

If nothing else, this gives us a baseline to work with, as Recorded Future continues to track ransomware attacks in these countries to understand their growth and hopefully encourage more research and analysis.

5. Publishing Victim Files Will Become More Popular

Already, the cybercriminals behind MAZE, REvil, Nemty, and DoppelPaymer have either threatened to release the files of victims who refuse to pay or have done so. On the surface, this makes sense as a tactic: if the victims won't pay the ransom, the attacker may be able to extort victims in other ways. But it remains to be seen whether this will be a successful extortion strategy for the ransomware actors. There have not been any reports of victims who refused to pay the ransom, or stopped the ransomware attack, turning around and coughing up money for extortion, and there is a good chance there won't be. This may be because victims don't want to admit to paying an extortion, or it could be because no victim has paid the extortion. There is strong distrust that the ransomware cybercriminals will actually delete the files after the extortion has been paid.

That doesn't mean that ransomware actors won't increasingly adopt this tactic. Public extortion garners a lot of media attention, which is something that many of these cybercriminals crave, at least in part to aid in the sales of their RaaS offerings by pointing to all of the coverage as a sign of success.

There is more risk for the cybercriminal in releasing the files, especially on a publicly accessible site, but at least in the short term, the perceived potential for reward will undoubtedly outweigh the risk.

This new tactic also highlights why early detection is so important in a ransomware attack. It is not enough to look for the ransomware itself — security teams have to be watchful for the tools the attackers are using to gain entry and explore the network. Alerting on, and quickly responding to, detections of Emotet, Trickbot, Mimikatz, or PSExec can stop the ransomware attack before the first system is encrypted.

Closing Thoughts

At this point, it's almost cliché to state that ransomware actors continue to evolve and improve their tactics, but that hasn't changed. The ransomware defenses of last year are not as effective against this year's attacks. Ransomware actors have gone from relying heavily on web exploitation against a wide range of targets to a combination of phishing and remote exploitation targeting primarily businesses, healthcare, and government agencies.

The cybercriminals behind ransomware are engaging in increasingly sophisticated operations against their targets. These attacks can sometimes take weeks from the initial exploitation until the ransomware is finally deployed.

If a ransomware attacker is sitting in your network for weeks before encrypting the first machine, that gives them ample time to exfiltrate gigabytes' worth of data, as we have repeatedly seen. Understanding the vulnerabilities that ransomware attackers are exploiting, how they are moving around the network, and the infrastructure they are using for command and control allows you to detect the attack before they can install ransomware and steal your data.

Using [security intelligence](#) to understand how ransomware attacks have evolved and are continuing to evolve can help your organization better deploy your defenses to match the current threat — not last year's threat.

About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.