RANSOMWARE IN A GLOBAL CONTEXT

VIRUSTOTAL

October 2021

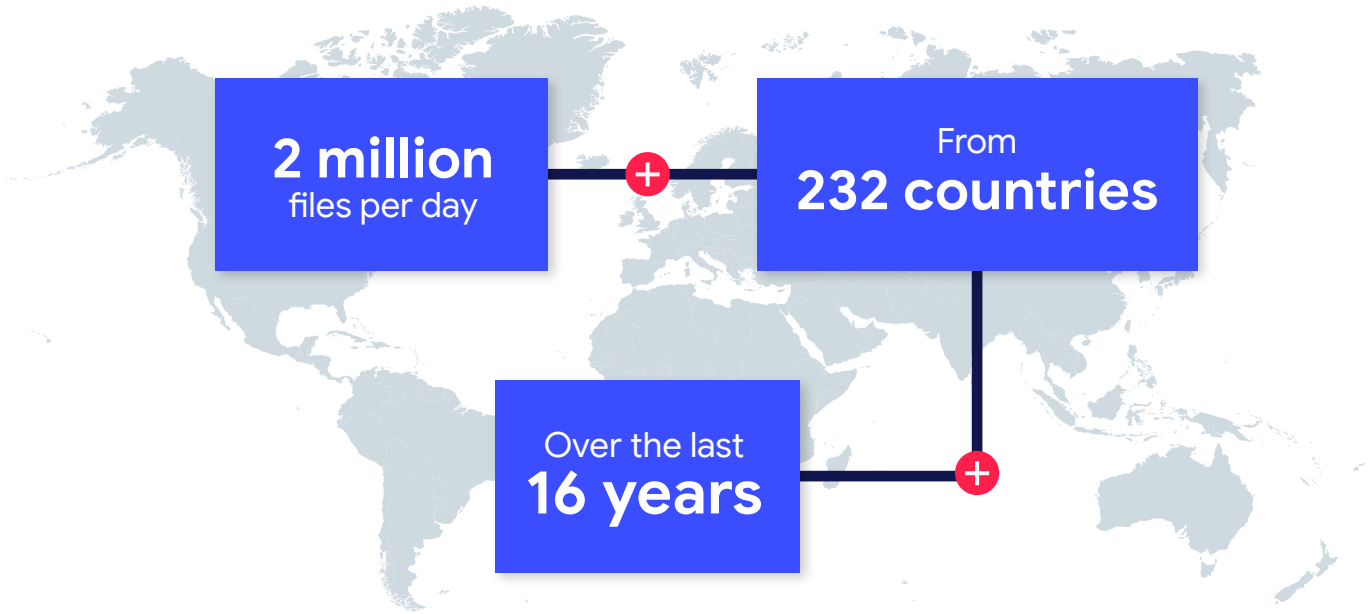
Welcome

Welcome to VirusTotal's first Ransomware Activity Report. This initiative is designed to help researchers, security practitioners and the general public better understand the nature of ransomware attacks by sharing VirusTotal's visibility.

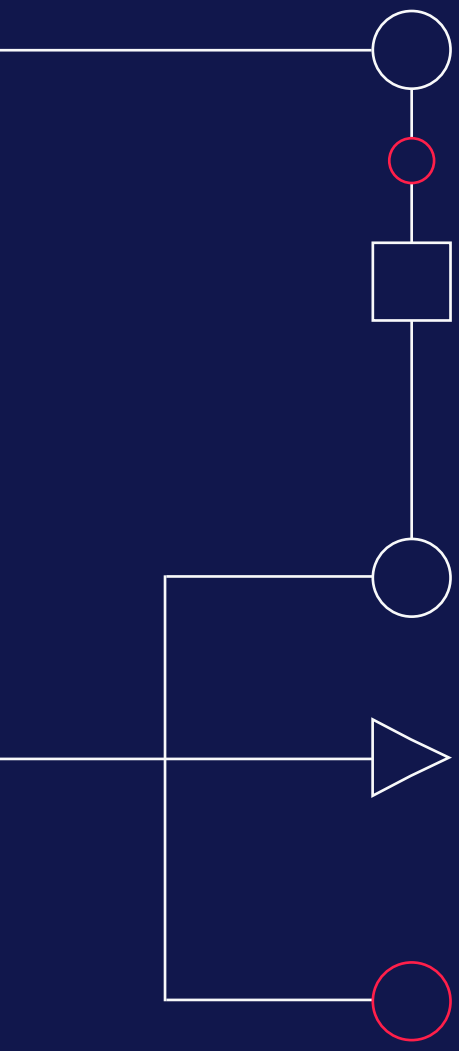
One of the main challenges for defenders is understanding the whole picture. We all have a partial view at best and it has proved difficult to condense and analyze significant and rich data in a single place.

This is where VirusTotal comes in. We are in a unique position to provide comprehensive visibility. **Over the last 16 years, we have processed more than 2 million files per day across 232 countries**. VirusTotal also harnesses the continuous contribution of its community of users to provide relevant context. We use this crowdsourced intelligence to analyze relevant data, share an understanding of how attacks develop, and help inform how they might evolve in the future.

This report is the first step in what we hope will become an ongoing community effort to discover and share actionable information on malware trends.



Executive Summary



Since 2020, users from more than **140 countries** have submitted ransomware samples to VirusTotal.

During this time, at least **130 different ransomware families** have been active.

Israel, South Korea, Vietnam, China, Singapore, India, Kazakhstan, Philippines, Iran and the UK are the 10 most affected territories based on the number of submissions to VirusTotal.

Activity among the most spread ransomware families comes and goes, but there is a baseline of activity of around 100 not-so-popular ransomware families that never stops.

According to our observations, it seems that in most cases attackers prepare fresh new samples for their campaigns.

In **July 2021** we observed a wave of the new variant of **Babuk** ransomware.

GandCrab was the most active family in early 2020, before its prevalence decreased dramatically in the second half of the year.

Methodology

VirusTotal relies on crowdsourced contributions and its vendor-independence. As such, it provides a valuable picture of how different attacks spread and evolve. All the data in this report is based on a subset of submissions from our users, as well as a number of different ransomware-related samples found in our databases dating back to January 2020.

Without applying any filters to the anti-virus verdicts data found in VirusTotal, we registered more than 80 million potential ransomware-related samples during this time period. In order to ascertain the most useful intelligence we filtered out the noise and focused on a smaller, curated and representative set of around 1 million double-checked ransomware samples[1].

[1] Sample confirmed to be ransomware-related by at least two different sources

Ransomware attacks: volume and spread

The figure below shows the distribution over time of ransomware-related submissions since January 2020:

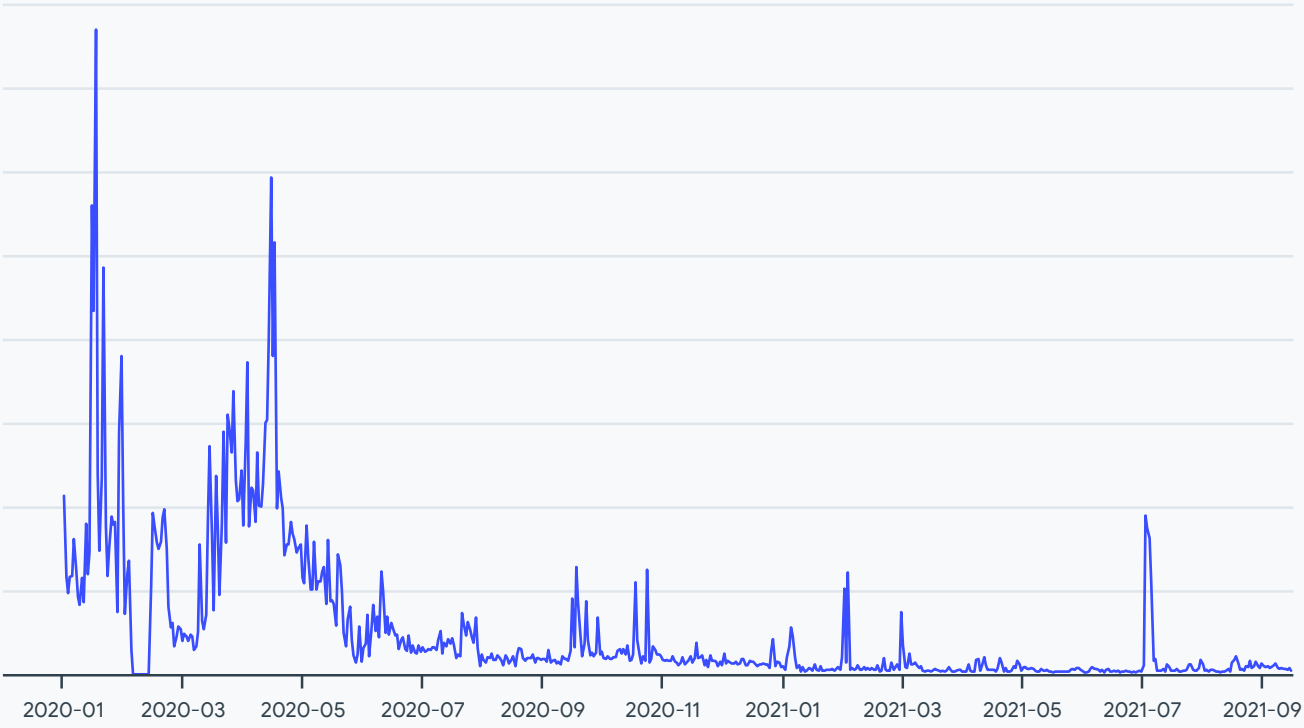


Fig 1.
Temporal distribution of ransomware-related submission

This graph shows the volume of the attacks. Note that a single sample can be submitted by multiple users.

The volume of submissions proved high in the first two quarters of 2020, showing some remarkable peaks. As we will explore later in this report, these peaks can be attributed to the GandCrab ransomware family which was extremely active at the time. Excluding GandCrab, there is a constant baseline showing several peaks, notably in Q1 2021, and another sizable peak around July 2021 that relates to the Babuk ransomware family.

Geographical distribution

In order to understand which countries were most affected, we examined the ransomware-related submissions during this period and excluded automatic submission systems which could distort the results.

The results were adjusted to account for the geographical distribution of our community. The following chart shows the percentage difference of submissions from a certain region compared to the regular geographical distribution of submissions:

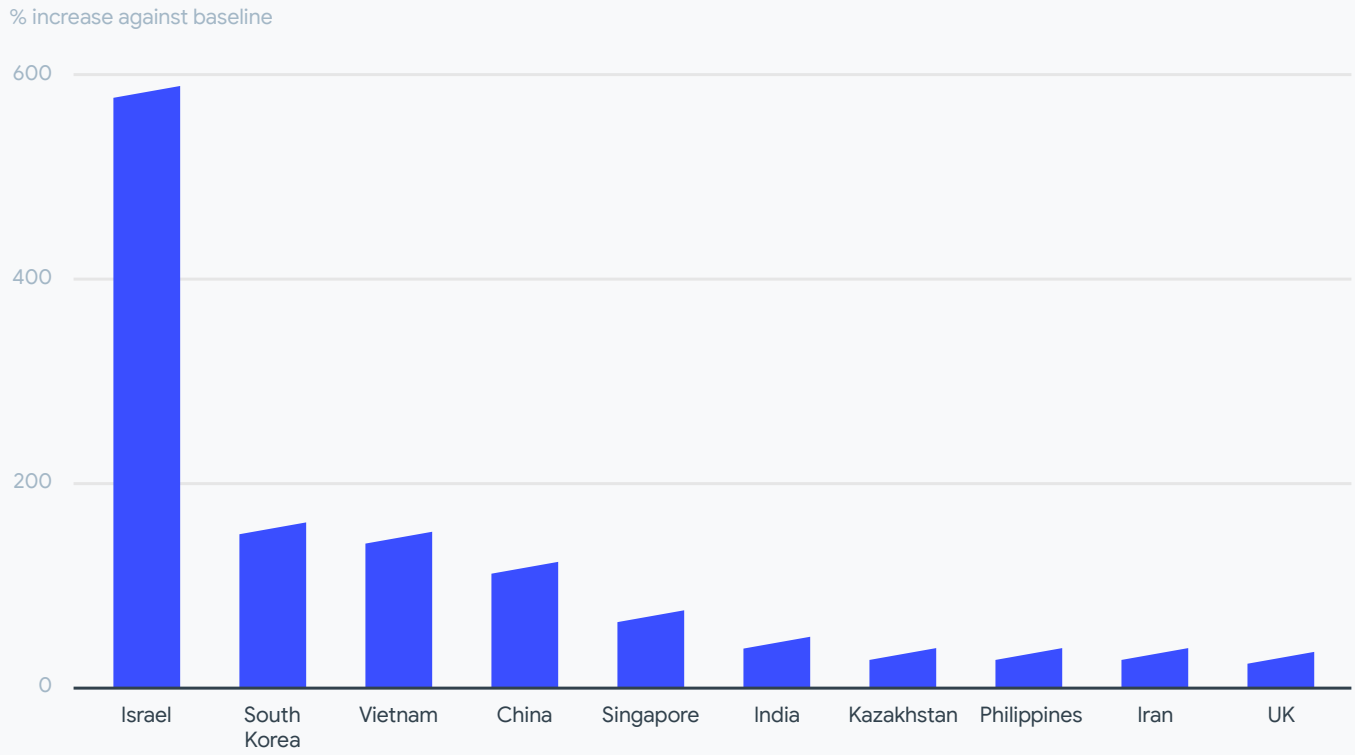


Fig 2.
Geographical distribution of ransomware-related submissions

Israel is the most noteworthy outlier, with nearly a 600 percent increase in the number of submissions compared to its baseline. It is followed by South Korea, Vietnam, China, Singapore, India, Kazakhstan, Philippines, Iran and the UK.

How fresh are the ransomware samples used in the attacks?

In examining when samples used in ransomware attacks were first seen on our platform, we can see there is a correlation between the both charts below:

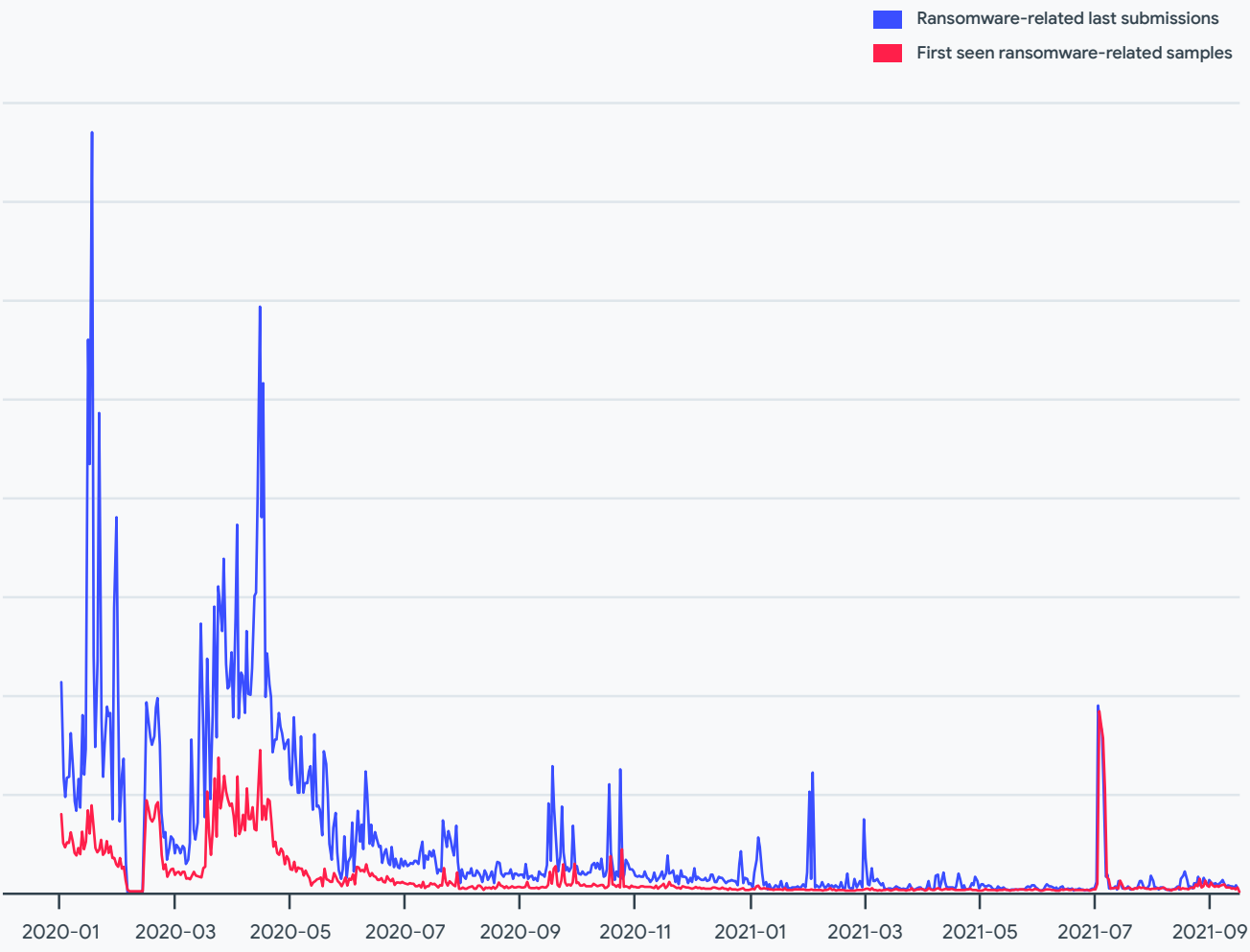


Fig 3.
Temporal distribution of ransomware-related last submissions and first seen ransomware-related samples

This could indicate that malicious actors prepare fresh new samples for most of their attacks. However, in other cases, such as the peaks we observed in Q1 2021, activity does not appear to be related to a new wave of freshly-created malware, but rather the reuse of a previous strain.

Ransomware families

In the course of our analysis, we identified at least 130 different ransomware families. Identification was not a trivial exercise given the different naming conventions used by the security industry. For example, the set of samples we selected for our analysis can be grouped into more than 30,000 different clusters based on similarity. Clusters are sets of malware grouped together because they look similar.

One way to understand how many distinct ransomware attacks the community faced at a given point of time is to display ransomware similarity clusters in a timeline.

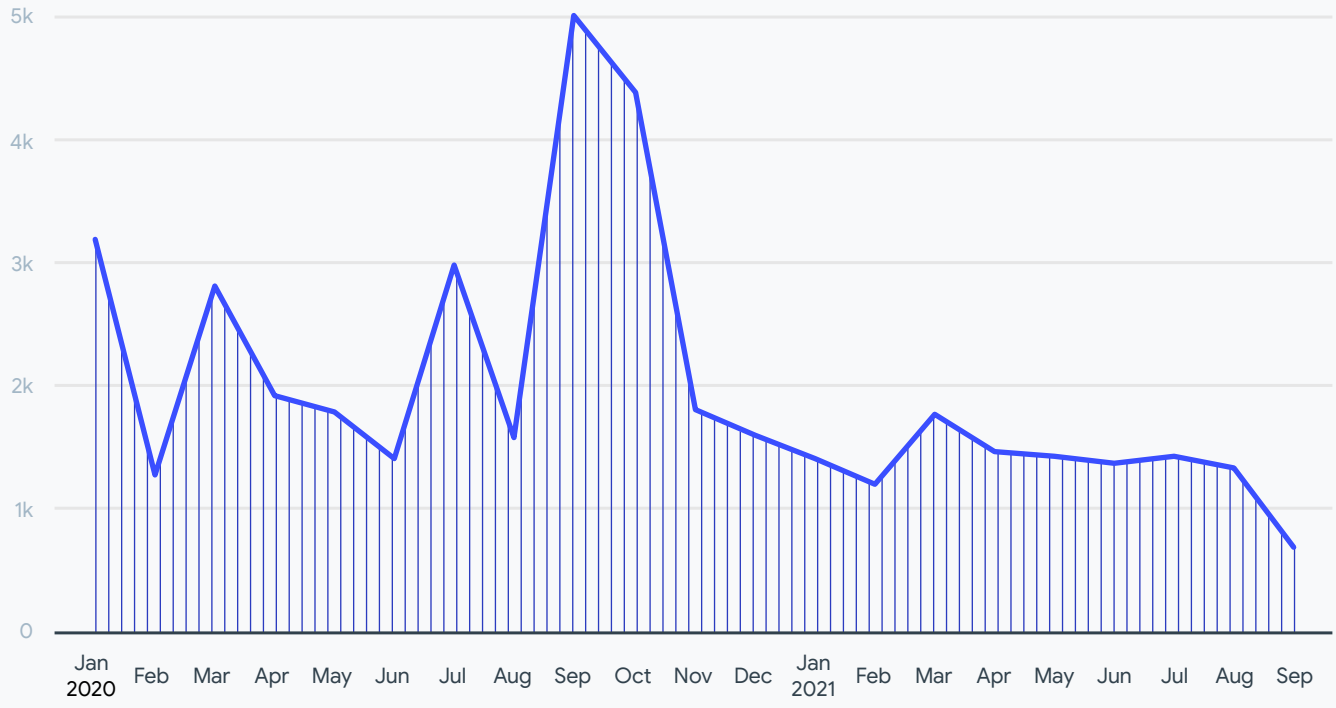


Fig 4.
Temporal distribution of ransomware-related clusters

In September 2020, for example, defenders had to monitor, detect and analyze around 5,000 clusters of samples.

It is worth noting that there is a baseline of between 1,000 and 2,000 first-seen ransomware clusters that is a constant presence throughout the period analyzed.

The following chart shows the number of ransomware clusters identified grouped by family.

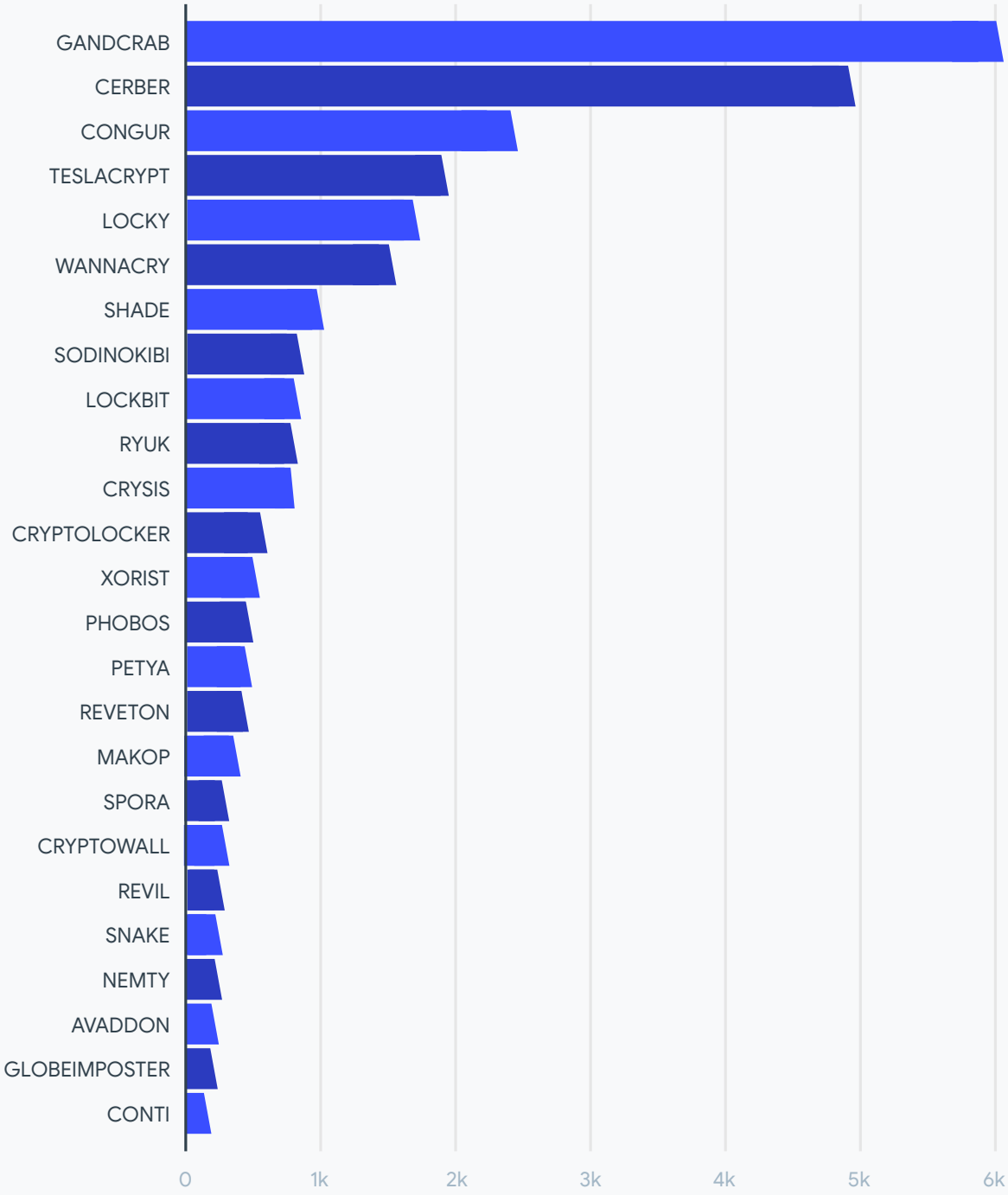


Fig 5.
Ransomware-related clusters per family

Where there is a high number of clusters associated with a single family, it speaks to the variety of malware used. This, in turn, can make detection harder.

Which are the most active ransomware families?

The following graph shows the top 10 ransomware families by number of different samples:

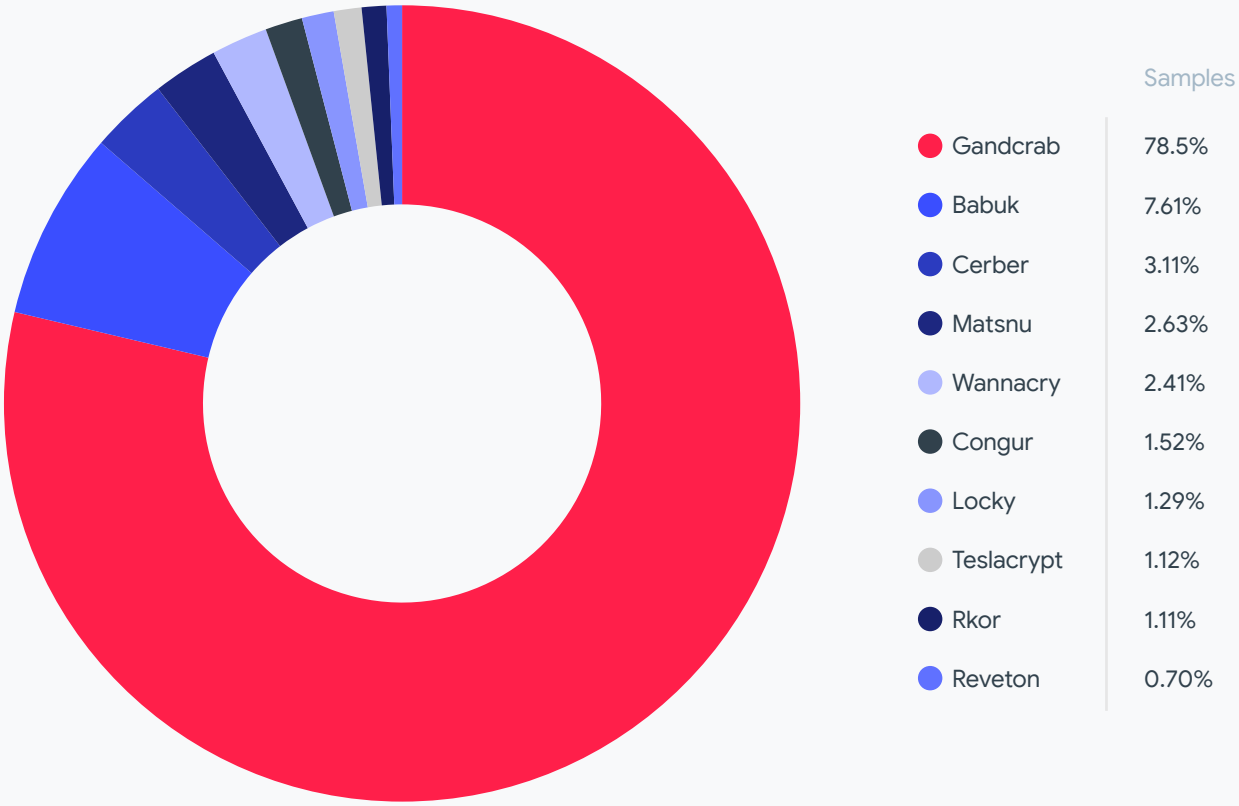


Fig 6.
Top 10 ransomware families by number of different samples

Among the top 10 ransomware families, we can see the presence of wannacry. This is probably a remnant of an old detection that still applies to some current ransomware families. However, we don't believe this points to any new wave of wannacry attacks.

The following chart shows the evolution of first-seen samples for the top 10 ransomware families:

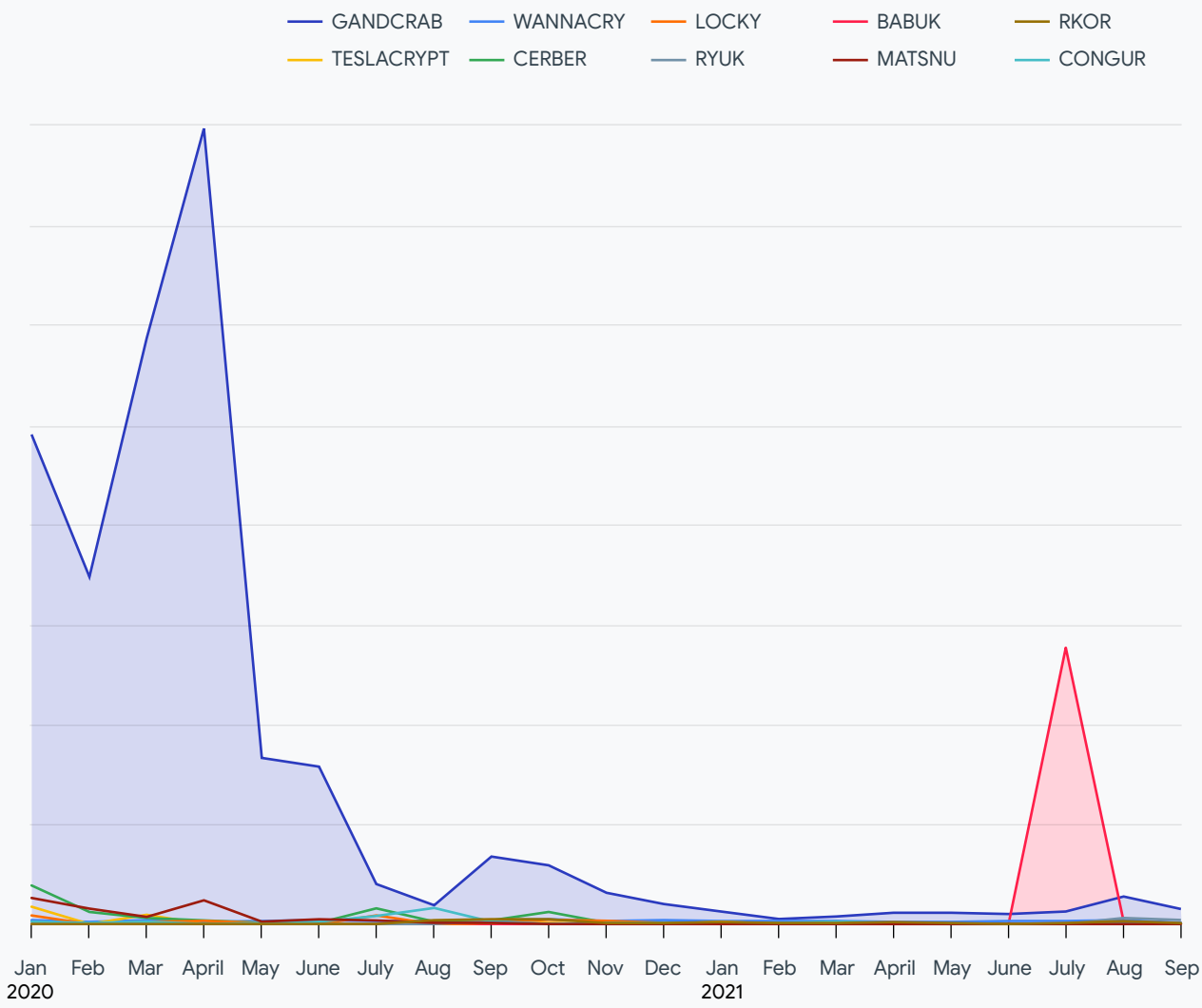


Fig 7.
Top 10 ransomware families temporal evolution by number of first seen samples

GandCrab had an extraordinary peak in Q1 2020 which dramatically decreased afterwards. It is still active but at a different order of magnitude in terms of the number of fresh samples.

Having an extreme outlier such as GandCrab makes the rest of families almost invisible in the chart with the exception of the Babuk ransomware peak in July 2021. To improve the visibility of the other top 10 ransomware families, we created a second chart that excluded GandCrab and Babuk:

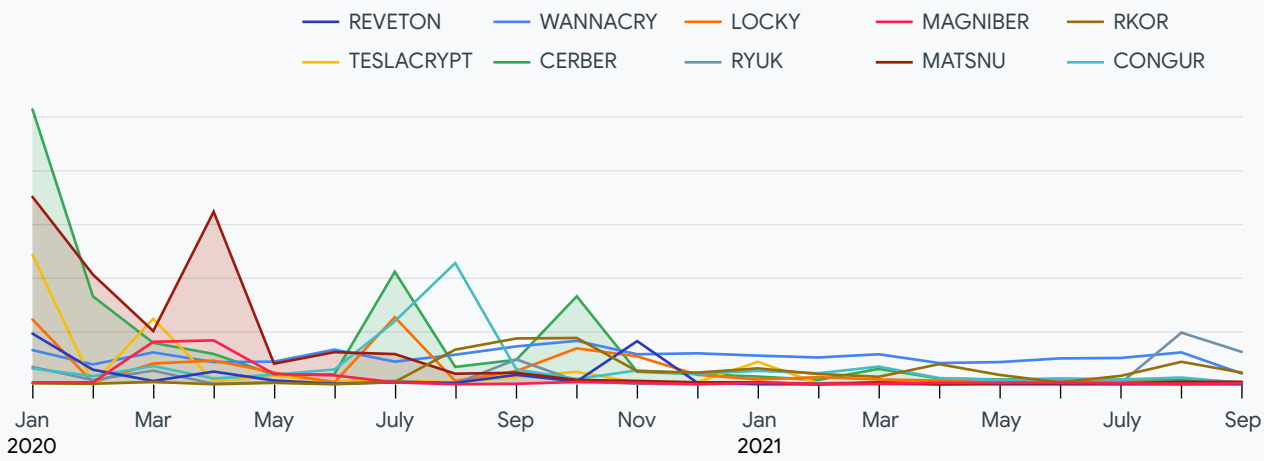


Fig 8.
Top 10 ransomware families temporal evolution by number of first seen samples excluding GandCrab and Babuk

For these eight ransomware families, sample peaks can be detected throughout 2020.

Beyond the top 10, there is constant activity among more than 100 other ransomware families. This baseline activity is overshadowed by the volumes associated with the most predominant families, but it is relevant nonetheless.

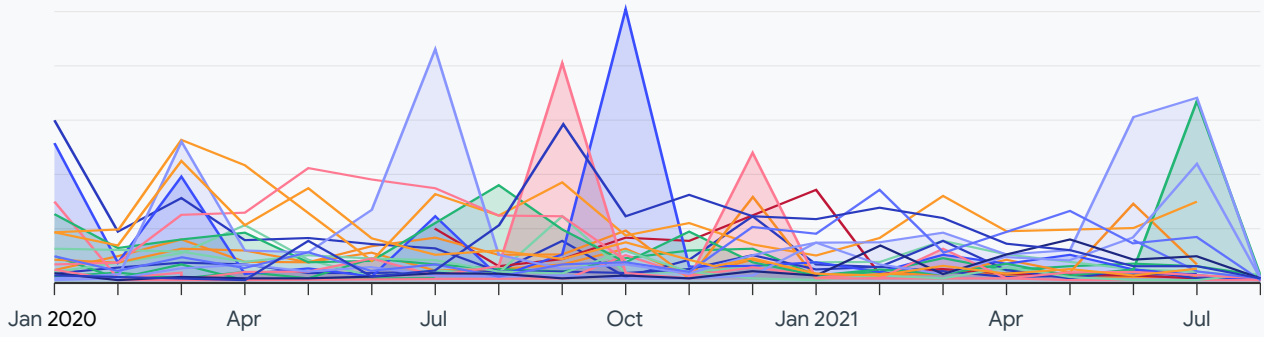


Fig 9.
Temporal evolution by number of first seen samples excluding top 25 families

A few considerations on technical sophistication

According to our study, 95 percent of ransomware files detected were Windows-based executables or dynamic link libraries (DLLs). Meanwhile, 2 percent were Android-based. It is worth highlighting a set of EvilQuest ransomware targeting OSX with the vast majority of samples first seen around mid-2020. Even when this set has approximately one million samples, they are all simple variations that can be grouped in 20 clusters.

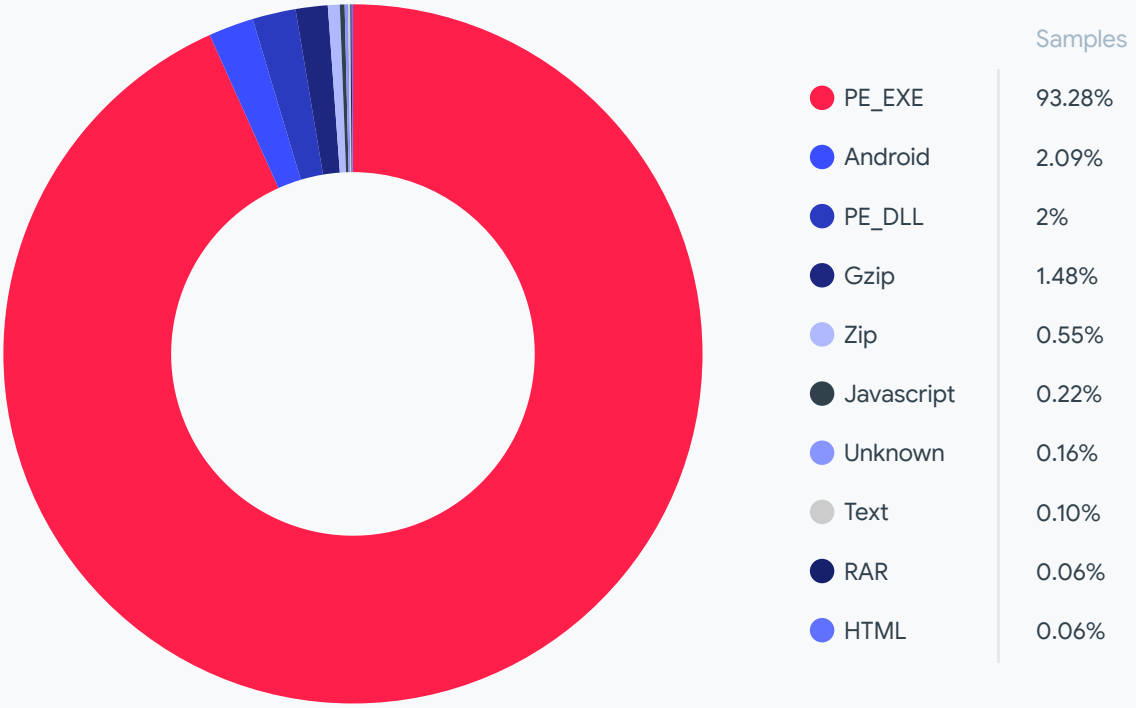


Fig 10.
Types of ransomware samples

According to our visibility off the kill chain, there are few samples directly associated with exploits. We believe this makes sense given that ransomware samples are usually deployed using social engineering and/or by droppers (small programs designed to install malware).

Around 5 percent of the analyzed samples were associated with exploits, most commonly Windows elevation of privileges and SMB information disclosures and remote execution. Only two of the top 10 exploited vulnerabilities were disclosed in 2020, and none in 2021.

Artifacts used for malware distribution

In some cases it was possible to associate artifacts used by attackers at some stage of the kill chain with ransomware families. We can divide these artifacts into two groups: those that might have been used to distribute ransomware and those used for lateral movement. In the distribution group these are the top five artifacts:

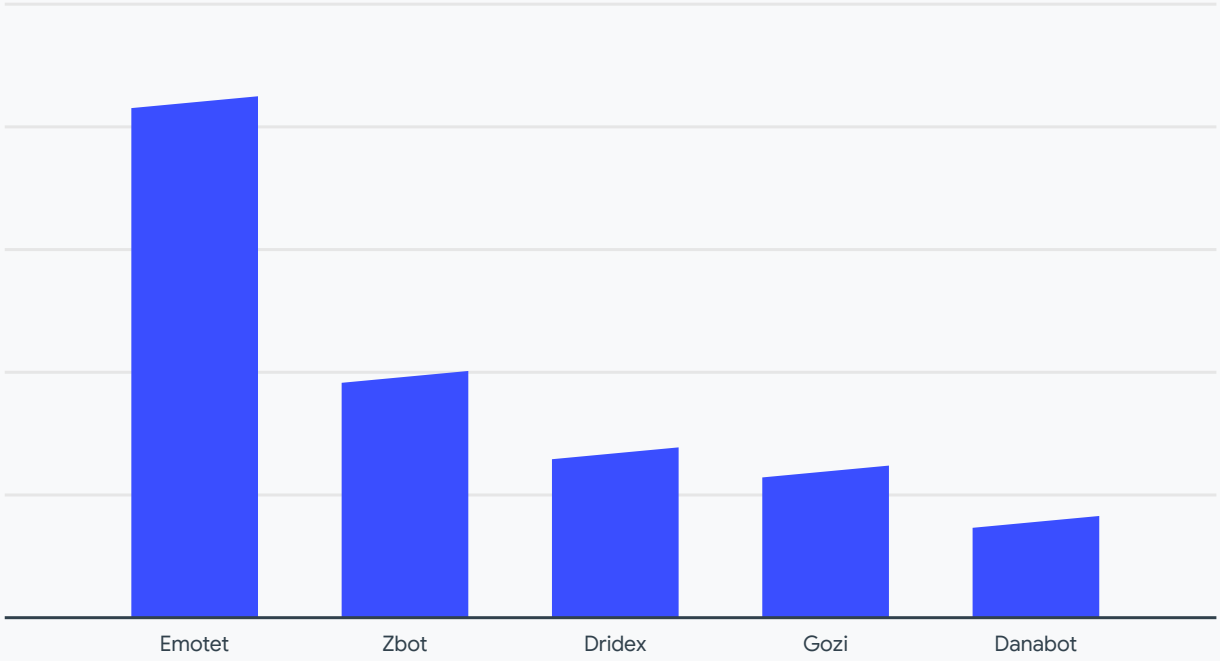
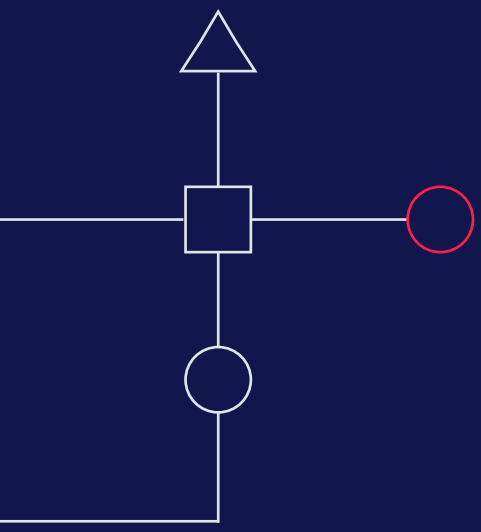


Fig 11.
Top artefacts used for distribution

These malware families are identifiable as being used by almost all of the top 10 ransomware families. However, we cannot confirm that attackers used any existing botnets for ransomware distribution.

In terms of artifacts used for other stages of the attack such as lateral movement, we identified the use of Mimikatz and Cobaltstrike, several scripting languages such as AutoIT and Powershell, and dozens of remote access Trojans (RATs) such as Phorpiex, Smokeloader, Nanocore, and Ponystealer.



Final thoughts

Working with such a large data set presented a number of challenges, starting with the simple consideration of whether or not a sample should be considered as ransomware. Is a single AV detection enough to define it as such? These kinds of decisions are the ones that every defender needs to make on a daily basis. In our case, we took advantage of using a platform providing multi-angular decision-making capabilities. Nevertheless, every security team must decide the best way to use the threat intelligence available. And, as a broad rule of thumb the more actionable data, the better.

As a side note YARA rules were not that effective to detect and classify ransomware unlike other malware activity. This is most likely because they are not updated as often as they are for other threats. This may also be due to the large amount of ransomware families active at the moment.

So what did we learn from our actionable data? Four things stand out

First, while big campaigns come and go, there is a constant baseline of ransomware activity that never stops.

Second, attackers are using a range of different approaches, including well-known botnet malware and other RATs.

Third, in terms of ransomware distribution attackers don't appear to need exploits other than for privilege escalation and for malware spreading within internal networks.

Finally, as noted earlier, Windows accounts for 95 percent of the ransomware targets, compared to 2 percent for Android.

Our takeaways

Based on our findings, here are five takeaways an effective anti-ransomware strategy could consider:

Detection of well-known distribution malware, such as botnets-related and RATs.

Ensure the patching strategy prioritizes all SMB and Windows privilege escalation vulnerabilities.

Internal monitoring and hardening the use of scripting languages and lateral movement tools.

Regularly monitor new waves of ransomware activity and make sure detection and mitigation techniques are in place, updating YARA rules for example.

In the event detection might fail, always implement cyber resilience and recovery strategies.

We wanted to share this data as a first step to an open, healthy discussion and to help researchers understand how to better protect against these threats. We trust the information shared in this report will prove useful - and that it will keep our world a little bit safer.

Join the discussion

@virustotal

VIRUSTOTAL

Find out more at:

virustotal.com