SECURELIST by Kaspersky

Ransomware by the numbers: Reassessing the threat's global impact

MALWARE REPORTS

23 APR 2021

Kaspersky has been following the ransomware landscape for years. In the past, we've published yearly reports on the subject: PC ransomware in 2014-2016, Ransomware in 2016-2017, and Ransomware and malicious crypto miners in 2016-2018. In fact, in 2019, we chose ransomware as the story of the year, upon noticing the well-known threat was shifting its attention to municipalities. In the 2010s, with campaigns like WannaCry and NotPetya, ransomware became mainstream news. However, starting in 2018, we began noticing something else: the statistics for the overall number of ransomware detections were on a steep decline. What was happening? Was ransomware, in fact, a dying species of malware?

For anyone following the news in the infosecurity community, this seemed unlikely. In 2019 and 2020, stories of ransomware attacks made front-page headlines, from Maze attacking LG to the infamous APT group Lazarus adding ransomware to its arsenal. In the United States alone in 2020, ransomware hit more than 2,300

government entities, healthcare facilities and schools, according to the security company Emsisoft.

So, what's the story?

Ransomware hasn't disappeared; the threat has just undergone a fundamental shift. Widespread ransomware campaigns have been replaced with highly targeted, destructive attacks, often aimed at large organizations. In addition, attackers appear to be more focused on exfiltrating data as well as encrypting it, i.e., siphoning off confidential information and threatening to make it public if the victims refuse to pay. All of this is done with the aim of launching fewer attacks, each with a far larger payout, rather than collecting smaller amounts from a massive number of victims.

In this report, we'll take a look at the numbers behind the ransomware threat from 2019 to 2020, what they mean — and what they foretell about ransomware's future.

Key findings

- In 2020, the number of unique users that encountered ransomware on their devices was 1,091,454, a decline from 1,537,465 in 2019.
- In 2019, the share of users targeted with ransomware among the overall number of users that encountered malware was 3.31%; this declined slightly in 2020 to 2.67%.
- The share of ransomware detections among the overall number of malware detections was 1.49% in 2019 and 1.08% in 2020.
- In both 2019 and 2020, WannaCry was the most frequently encountered crypto-ransomware family on Windows systems.
- In 2019, the number of unique users that encountered ransomware on their mobile devices was 72,258. This number declined to 33,502 in 2020.
- However, the share of unique users that encountered ransomware on their mobile devices among the overall number of users that encountered malware held steady between 2019 and 2020 at 0.56%.
- From 2019 to 2020, the number of unique users affected by targeted ransomware families increased by 767%.
- By far, the industry that contained the greatest share of targeted ransomware attacks was engineering and manufacturing, at 25.63%.

Methodology

This report has been prepared using depersonalized data processed by Kaspersky Security Network (KSN).

There are two main metrics used. The first, unique users, refers to the number of distinct users of Kaspersky products with the KSN feature enabled who encountered ransomware at least once in a given period. The second is detections, which is the number of ransomware attacks blocked by Kaspersky products over a given period.

The report also includes research into the threat landscape by Kaspersky experts.

Kaspersky products detect various types of ransomware. These include crypto-ransomware (malware that encrypts your files), screen lockers, browser lockers, and boot lockers. Unless otherwise stated, statistics refer to any type of ransomware.

Ransomware across all platforms

As Kaspersky has previously noted, the total number of ransomware detections has been steadily declining since 2017. This is a trend that has continued through 2019 and 2020.

In 2019, the total number of unique users that encountered ransomware across all platforms was 1,537,465. In 2020, that number fell to 1,091,454 — a decrease of 29%.

Side-by-side comparison of the number of unique KSN users that encountered ransomware on their devices, 2019 – 2020 (download)

In fact, for each month in 2020, the number of unique users that encountered ransomware across all devices was lower than the number observed during the same month in the previous year. In both years, the number of users that encountered ransomware was relatively stable — hovering between 100,000 and 170,000 in 2020 and between 150,000 and 190,000 in 2019 — with the exception of July 2019, when there was a noticeable spike. This was driven by an increase in two ransomware families. The first, Bluff, is a browser locker, meaning victims are confronted with a fake tab — one they are unable to exit out of — that threatens dire consequences if a certain amount of money is not paid. The other was Rakhni, a crypto-ransomware that first appeared in 2013 and was distributed primarily through spam with malicious attachments.

The share of unique users that encountered ransomware out of the total number that encountered any type of malware across their devices also declined, from 3.31% in 2019 to 2.67% in 2020. However, the share of ransomware detections out of the total number of malware detections held relatively steady, declining only slightly from 2019 to 2020, from 1.49% to 1.08%.

The most active crypto-ransomware families

Three years after it first made headlines everywhere, WannaCry is still the most active crypto-ransomware family. To date, WannaCry is the largest ransomware infection in history, with damage totaling at least $4 billion across 150 countries. In 2019, 21.85% of users that encountered crypto-ransomware encountered WannaCry.

Top five crypto-ransomware families, 2019 (download)

Among other active families were GandCrab, a ransomware family that was active in 2019 and followed the RaaS model, STOP/DJVU, and PolyRansom/VirLock. Shade, a widespread cryptor that first appeared in 2014, was still one of the most active ransomware families in 2019, but its activity has been on the decline for years. In fact, in 2020, Kaspersky released a decryptor for all strains of Shade — and it was no

longer one of the five most active ransomware families detected by Kaspersky products.

Top five crypto-ransomware families, 2020 (download)

In 2020, WannaCry was still the most frequently encountered family, with 16% of users (80,207) that encountered crypto-ransomware encountering this malware. In addition, a new strain entered the top five most active families: Crysis/Dharma. Crysis is able to use multiple attack vectors, although recently it has primarily exploited unsecured RDP access. First discovered in 2016, the malware has continued to evolve and is now following ransomware-as-a-service model.

In general, 2019 and 2020 continued a trend first noticed in early 2018: the consolidation of ransomware groups. Only a few notable families continue to maintain a significant presence across the threat landscape, with the rest of attacks conducted by ransomware Trojans that do not belong to any specific family. Of course, new families do continue to appear, with STOP and GandCrab serving as excellent examples.

Geography of ransomware attacks

When analyzing the geography of attacked users, we take into consideration the distribution of Kaspersky's customers. That's why, when examining the geography of attacks, we use the percentage of users attacked with ransomware as a proportion of users attacked with any kind of malware in those regions where there are more than 10,000 unique users of Kaspersky products.

All percentages reflect the percent of unique users that encountered ransomware at least once on any device out of the total number of unique users that encountered any type of malware over the stated period.

Middle East

In 2019, the countries with the greatest share of users that encountered ransomware on any device in the Middle East were as follows:

Country	%*
Pakistan	19.03%
Palestine	6.74%
Yemen	6.55%
Egypt	6.41%
Iraq	6.28%

**Share of users attacked with ransomware out of all users encountering malware in the country*

Pakistan had, by far, the greatest share of users encountering ransomware: 19.03%. The other countries in the top five all had a share of roughly 6% of users that encountered ransomware.

In 2020, the five countries with the greatest share of users encountering ransomware remained the same with a few small adjustments.

Country	%*
Pakistan	14.88%
Yemen	7.49%
Egypt	6.45%
Palestine	5.48%
Iraq	5.37%

**Share of users attacked with ransomware out of all users encountering malware in the country*

Pakistan still had the greatest share of users, but the overall percentage declined to 14.88%. The percent of users encountering ransomware in Yemen actually increased to 7.49%, while the percentage of users in Palestine and Iraq lowered, and the share of affected Egyptians remained pretty much the same.

North and South America

In 2019, the countries in North and South America with the greatest percentage of users that encountered ransomware were the following:

Country	%*
United States	5.49%
Paraguay	4.87%
Venezuela	3.34%
Canada	3.25%
Guatemala	2.81%

**Share of users attacked with ransomware out of all users encountering malware in the country*

The United States had the greatest share at 5.49% percent, followed by Paraguay at 4.87%. Rounding out the countries with the greatest share of users encountering ransomware were Venezuela, Canada, and Guatemala.

In 2020, the countries with the greatest share in North and South America were mostly the same — although with a smaller percentage of users encountering ransomware.

Country	%*

United States	2.97%
Venezuela	2.49%
Canada	2.46%
Paraguay	2.44%
Uruguay	2.37%

**Share of users attacked with ransomware out of all users encountering malware in the country*

year, Venezuela had the second greatest share of users encountering ransomware, with Paraguay falling to fourth. In addition, Guatemala was replaced by Uruguay.

Africa

In 2019, the countries in Africa with the greatest percentage of users encountering ransomware were the following:

Country	%*
Mozambique	12.02%
Ethiopia	8.57%
Ghana	5.75%
Angola	3.32%
Libya	3.28%

**Share of users attacked with ransomware out of all users encountering malware in the country*

Mozambique had the greatest share of users by far at 12.02%, followed by Ethiopia at 8.57%. The remaining countries with the greatest percentage of users that encountered ransomware were Ghana, Angola, and Libya.

In 2020, the landscape shifted a bit:

Country	%*
Cameroon	6.83%
Mali	5.85%
Mozambique	5.62%
Ethiopia	5.39%
Ghana	3.85%

**Share of users attacked with ransomware out of all users encountering malware in the country*

The country with the greatest share of users encountering ransomware was Cameroon, followed by Mali. Mozambique, Ethiopia, and Ghana remained in the top five, but the share of users facing ransomware declined for all three.

Asia

In Asia in 2019, the five countries with the greatest percentage of users encountering ransomware were the following:

Country	%*
Afghanistan	26.44%
Bangladesh	23.14%
Turkmenistan	11.28%
Uzbekistan	10.53%
Tajikistan	8.08%

**Share of users attacked with ransomware out of all users encountering malware in the country*

Afghanistan had the greatest share of users at 26.44%, followed by Bangladesh at 23.14%. The next three countries with the greatest share of users were concentrated in Central Asia: Turkmenistan, Uzbekistan, and Tajikistan.

In 2020, the landscape slightly changed:

Country	%*
Afghanistan	17.67%
Bangladesh	11.31%
Turkmenistan	9.52%
Tajikistan	5.26%
Kyrgyzstan	4.05%

**Share of users attacked with ransomware out of all users encountering malware in the country*

Uzbekistan left the rating of countries with the greatest share of users encountering ransomware, giving way to Kyrgyzstan (4.05%), and the percentages of all the rest were significantly lower than in 2019. Afghanistan's share of users declined to 17.67% and Bangladesh's to 11.31%.

Europe

In Europe, the countries with the greatest percentage of users encountering ransomware were the following:

Country	%*
Azerbaijan	5.03%
Turkey	3.03%
Cyprus	2.82%
France	2.74%

Armenia	2.54%
Bulgaria	2.54%

**Share of users attacked with ransomware out of all users encountering malware in the country*

Azerbaijan had the greatest share at 5.03%, followed by Turkey and Cyprus. Rounding out the six countries with the greatest percentage of users encountering ransomware were France, Armenia, and Bulgaria, the last two having the same share of affected users.

In 2020, the landscape looked a bit different:

Country	%*
France	5.18%
Montenegro	4.36%
Monaco	4.22%
Azerbaijan	4.21%
Macedonia	4.06%

**Share of users attacked with ransomware out of all users encountering malware in the country*

France had the greatest share of users encountering ransomware, followed by Montenegro and Monaco, which replaced Turkey and Cyprus. Azerbaijan had the fourth greatest share at 4.21%, and Macedonia took Armenia's place as the country with the fifth greatest share.

Mobile ransomware

As is the case with ransomware across all devices, mobile ransomware continues to decline. In 2019, the total number of unique Kaspersky users that encountered ransomware was 72,258. In 2020, it was 33,502 — a decrease of 54%.

However, the share of mobile users that encountered ransomware out of the total number that encountered any type of malware remained steady at 0.56%. This coincided with a decline in the overall number of mobile ransomware detections — from 333,878 in 2019 to 290,372 in 2020.

Number of mobile ransomware detections from 2019 to 2020 (download)

Interestingly enough, while the number of mobile ransomware detections declined relatively steadily after July 2019 with just a few small spikes in July 2019 and February 2020, it again started to rise significantly in the second half of 2020, reaching 35,000 detections in September of last year. This was due to, oddly enough, the ransomware Encoder, which is actually designed for Windows workstations and is not dangerous for mobile devices. However, in September 2020, Encoder spread

via Telegram, which has both a mobile and desktop application. The attackers were most likely targeting Windows users, and mobile users accidentally ended up with Encoder on their phones when the mobile version of Telegram synced downloads with the desktop client.

Most active mobile ransomware families

Distribution of the most active mobile ransomware families, 2019 (download)

In 2019, nearly 45% of users that encountered mobile ransomware encountered Svpeng, the family that started as SMS Trojans, then switched to stealing banking credentials and credit card data, and finally evolved into ransomware. Slightly less than 19% of users encountered Rkor and Small. Rkor is a classic locker for ransom. Distributed via porn, it uses accessibility services to gain the necessary control over a device and then locks it until a fee is paid. Small is very similar: it locks the screen and demands a fee to continue watching porn.

The fourth most common family is Congur, which is distributed via a modified application, such as WhatsApp. Another well-known active family is Fusob, which claims to be from some kind of authority and says that the intended victim is obligated to pay a fine.

Distribution of the most active mobile ransomware families, 2020 (download)

In 2020, Small was the most frequently encountered mobile ransomware family at 26% followed by Rkor and Congur. Svpeng was the fourth most common family, with 14% of users encountering it.

Geography of attacked users

In 2019, the countries with the greatest percentage of users that encountered ransomware on their mobile devices were the following:

Country	%*
United States	33.19%
Kazakhstan	13.24%
Canada	2.71%
Germany	2.27%
Italy	2.19%
United Kingdom	1.53%
Iran	1.41%
Poland	1.22%
Mexico	1.09%

Spain	1.00%

**Share of users attacked with ransomware out of all users encountering malware*

The countries with the greatest number of users encountering mobile ransomware were relatively dispersed globally, with the United States having the highest percentage. Kazakhstan followed at 13.24%. The rest of the top ten had significantly smaller percentages of users encountering mobile ransomware, with Canada — the country with the third largest share — having only 2.71%.

In 2020, the countries with the greatest percentage of users that encountered mobile ransomware were the following:

Country	%*
Kazakhstan	23.80%
United States	10.32%
Germany	2.54%
Egypt	1.46%
Mexico	1.43%
Italy	1.41%
United Kingdom	1.14%
Iran	1.07%
Malaysia	1.02%
Indonesia	1.01%

**Share of users attacked with ransomware out of all users encountering malware*

In 2020, Kazakhstan had the greatest percentage of users encountering mobile ransomware at 23.80%, followed by the United States at 10.32%. Poland, Spain, and Canada were replaced by Malaysia, Indonesia, and Egypt. In general, the percentage of affected users declined — this is to be expected given that the overall number of users affected by mobile ransomware declined by more than 50%.

The rise of targeted ransomware

While the raw total of ransomware detections has been on the decline, those numbers only tell part of the story. When ransomware first made front-page headlines, it was because of campaigns like WannaCry, Petya, and CryptoLocker: massive campaigns interested in hitting as many users as possible and extorting relatively small amounts per user. In WannaCry, for example, the attackers only requested $300 and later raised this amount to $600.

However, these types of campaigns are becoming less profitable, for potentially several reasons. Given the increasing amount of attention paid to ransomware, security software may have become better at blocking ransomware threats and people are repeatedly encouraged not to pay. In addition, in a lot of countries, people

simply can't afford that high of a ransom. As a result, attackers have shifted their focus to those who can pay — companies. In 2019, nearly one-third of victims targeted by ransomware were corporate users.

Of course, infecting companies requires a far more sophisticated, targeted approach, and there are specific ransomware families designed to do just that.

Targeted ransomware (also known as "big game hunting") consists of families of ransomware used to extort money from a particular victim. These victims tend to be high profile, such as large corporations, government and municipal agencies, and healthcare organizations, and the ransom demanded is far larger than that demanded from separate users. Often, their attacks involve one or more of the following stages:

- Network compromise
- Reconnaissance & persistence
- Lateral movement
- Data exfiltration
- Data encryption
- Extortion

Initial infection often occurs via exploitation of server-side software (VPNs, Citrix, WebLogic, Tomcat, Exchange, etc), RDP brute-force attacks/credential stuffing, supply-chain attacks, or botnets.

Kaspersky classifies a particular ransomware group as "targeted" based on the victims chosen, and if sophisticated methods are used to conduct the attack, such as breaching the network or lateral movement. So far, Kaspersky has identified 28 of these targeted families, which includes the infamous Hades ransomware that targets companies worth at least $1 billion.

From 2019 to 2020, the number of unique users affected by targeted ransomware — ransomware that is designed to affect specific users — increased from 985 to 8,538, a 767% jump.

The number of unique Kaspersky users affected by targeted ransomware, 2019 – 2020 (download)

A major spike occurred in July 2020, which was driven by the REvil ransomware family, which successfully exploited the foreign exchange company Travelex for $2.3 million. Grubman Shire Meiselas & Sacks, a New York-based law firm with a host of celebrity clients, also fell victim to REvil in May. Other highly targeted ransomware families also appeared in 2019 and 2020, the most notable of which was Maze. First appearing in 2019, Maze used various mechanisms for initial compromise. In certain cases, they used spear-phishing campaigns to install Cobalt Strike RAT, while other attacks involved exploiting a vulnerable internet-facing service (e.g., Citrix ADC/NetScaler or Pulse Secure VPN) or weak RDP credentials to breach the network. Maze primarily targeted businesses and large organizations. Some of their most notable attacks were against LG and the city of Pensacola, Florida.

Alongside this rise in targeted ransomware there has been an increased focus not just on data encryption but on data exfiltration: searching for highly confidential information and threatening to make it public if the ransom isn't met as a means of coercing organizations to pay. Maze was one of the first ransomware groups to actually publish this stolen data if the ransom wasn't paid. In addition, this information can later be sold online at auctions, which is what happened with databases from various agricultural companies that had fallen victim to REvil in the summer of 2020.

Eventually, Maze teamed up with another well-known, highly targeted ransomware family, RagnarLocker, which first appeared in 2020. Like Maze, RagnarLocker targets primarily large organizations and publishes the confidential information of those who refuse to pay on the "Wall of Shame." This family is so targeted that each individual malware sample is specifically tailored to the organization it is attacking.

WastedLocker also appeared in 2020 and made global headlines when it knocked most popular services by Garmin, the well-known fitness and GPS technology company, offline for three days as it held the company's data for a $10 million ransom. The malware used in the attack was specifically designed for Garmin.

Targeted ransomware is not confined to one specific industry. It has affected everything from healthcare organizations to sports and fitness companies.

Distribution of targeted ransomware attacks by industry, 2019–2020 (download)

Engineering and manufacturing was the most represented industry by far, with 25.63% of targeted ransomware attacks from 2019 to 2020 affecting this industry. This is not surprising given the highly sensitive nature of their data and the often high value of such companies. It is also incredibly disruptive to businesses in this sector if their systems go offline. 7.60% of targeted ransomware attacks affected professional and consumer services companies, and 7.09% targeted financial firms. Other popular targets are construction & real estate, commerce & retail, and IT & telecommunications.

Conclusion

The world is entering a new era of ransomware, and it's likely that any kind of large-scale campaign — the kind that targets average, everyday users — will be few and far between. Of course, that's not to say ransomware is only a threat if you're a large company. Just in December of last year, there was a group looking to capitalize on the launch of Cyberpunk 2077 by distributing a fake, mobile version of the game that encrypts users' files once downloaded.

That said, there has been an unmistakable shift in the landscape — one aimed at extorting confidential information and recovering large sums of money by targeting just one or maybe a dozen organizations. That means ransomware attackers will continue to deploy more advanced techniques for infiltrating networks and encrypting data. APT groups like Lazarus have already begun adding ransomware to

their toolset. It wouldn't be surprising if additional advanced threat actors followed suit.

The biggest takeaway from this is that companies — large and small — need to think about more than just backing up their data. They need to take a comprehensive approach to their security — one that includes regular patching, software updates, and cybersecurity awareness training. Some of these attacks against companies involve gaining an initial foothold in the system, laterally moving throughout the network until full control has been achieved, and then conducting reconnaissance for months before striking at a moment that causes optimal damage. In the attack against Travelex with the REvil ransomware, the cybercriminals had infiltrated the company's network six months before they actually encrypted the data and demanded the ransom.

Ransomware attackers are sharpening their toolsets, and companies need to respond in kind. Fortunately, doing so is completely within their power.

Here are just a few suggestions from Kaspersky experts on the ways you can safeguard your organization against ransomware:

1. Always keep software updated on all the devices you use to prevent ransomware from exploiting vulnerabilities.
2. Focus your defense strategy on detecting lateral movements and data exfiltration to the internet. Pay special attention to the outgoing traffic to detect cybercriminals' connections. Back up data regularly. Make sure you can quickly access it in an emergency when needed.
3. Use solutions like Kaspersky Endpoint Detection and Responseand Kaspersky Managed Detection and Response, which help identify and stop an attack at an early stage, before attackers reach their final goals.
4. To protect the corporate environment, educate your employees. Dedicated training courses can help, such as the ones provided in the Kaspersky Automated Security Awareness Platform. A free lesson on how to protect your business from ransomware attacks is available here.
5. Use a reliable endpoint security solution, such as Kaspersky Endpoint Security for Business, which is powered by exploit prevention, behavior detection, and a remediation engine that is able to roll back malicious actions. KESB also has self-defense mechanisms that can prevent its removal by cybercriminals.