kaspersky

Ransomware 2018-2020

Ransomware is a threat all too familiar to the cyber security industry. Its families and activities were well reported by various tech communities after the ransomware pandemic in the second half of the 2010s. This includes Kaspersky, which has a long tradition of reporting on the evolution of ransomware – you can find previous reports on the threat here, here, and here.

For years, this malware was a particularly pernicious problem for the cybersecurity world, infecting and blocking access to thousands of devices and files and requiring users to pay a ransom (usually in e-currency) if they wanted to regain access to their important information.

However, closer to the end of the decade, it seemed as if the prevalence of this type of malware had declined—apparently due to public attention.

Yet several events from the beginning of 2020 suggest that ransomware is still a persistent threat—even if not as widespread.

In February, a major US natural gas facility had to shut down one of its pipelines for two days after an undisclosed type of ransomware malware infected its systems.

Europe’s energy sector was then hit in April of this year when Energias de Portugal (EDP), one of the fourth largest European energy operators, was attacked by the Ragnar Locker malware. The attackers claimed they had stolen 10 TB of sensitive information, which they would only return if given 10 million Euros in bitcoin.

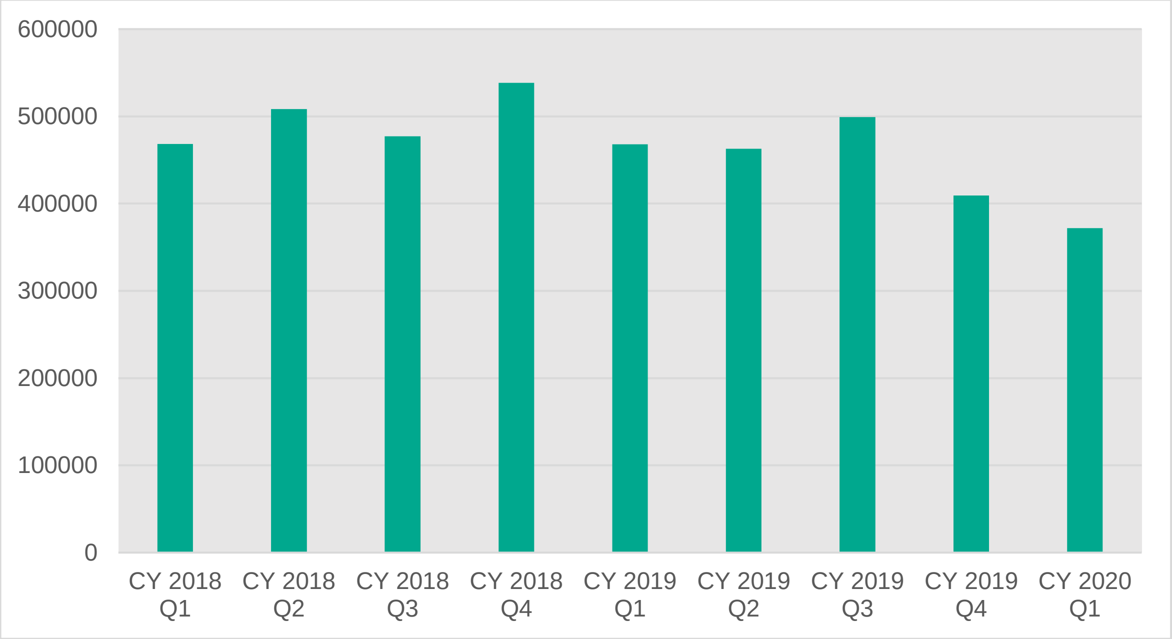
Perhaps most alarmingly, cyber criminals have taken advantage of the current pandemic to launch ransomware attacks against the healthcare sector. In March, a major COVID-19 testing lab in Europe was hit, and in April, a hospital in Colorado, USA was unable to use its system for storing patient information after an assault in April. Last month, INTERPOL released a statement warning healthcare institutions about the growing threat of ransomware and urged them to take precaution.

Given these recent events—and the fact that the threat is still actively evolving, with new families being created and different industries being targeted—we decided the ransomware landscape deserved a closer look. The data below reflects ransomware activity from 2018 to the first months of 2020. The text has been prepared using depersonalized data processed by Kaspersky Security Network (KSN).

The metrics are based on the number of distinct PC users of Kaspersky products that have the KSN feature enabled who encountered ransomware at least once in a given period, as well as research into the threat landscape by Kaspersky experts.

2018-2020 Q1 in figures

The figures for the observed period demonstrate a fluctuating rate of attacks—with spikes during certain quarters. Over the entire period—January 2018 to March 2020—**3.8%** of all users that encountered malware, encountered ransomware.



The number of unique users encountering ransomware at least once from January 2018 to March 2020

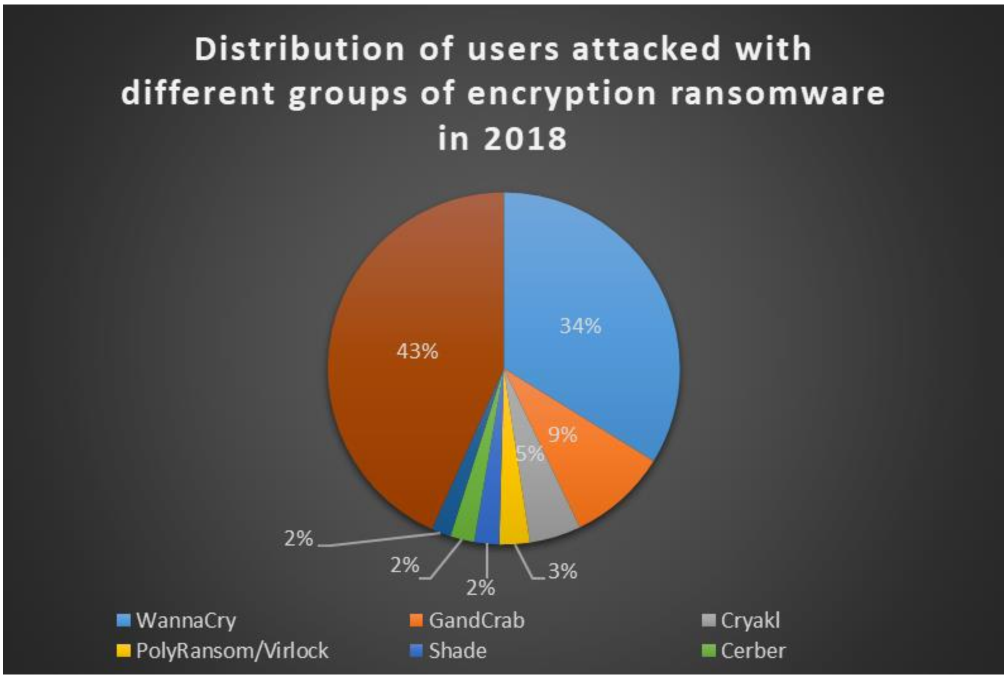
Between 2018 and 2019, the total number of users that encountered ransomware declined slightly—from **1,681,867** from January-December of 2018 to **1,554,669** from January-December of 2019 (a **7.6% decrease**).

Additionally, the first quarter of 2020 reported the lowest number of users that encountered ransomware than any quarter of the previous two years. It appears to follow the general trend of a quarter-by-quarter decline beginning in the first quarter of 2019 (with the exception of July-September 2019).

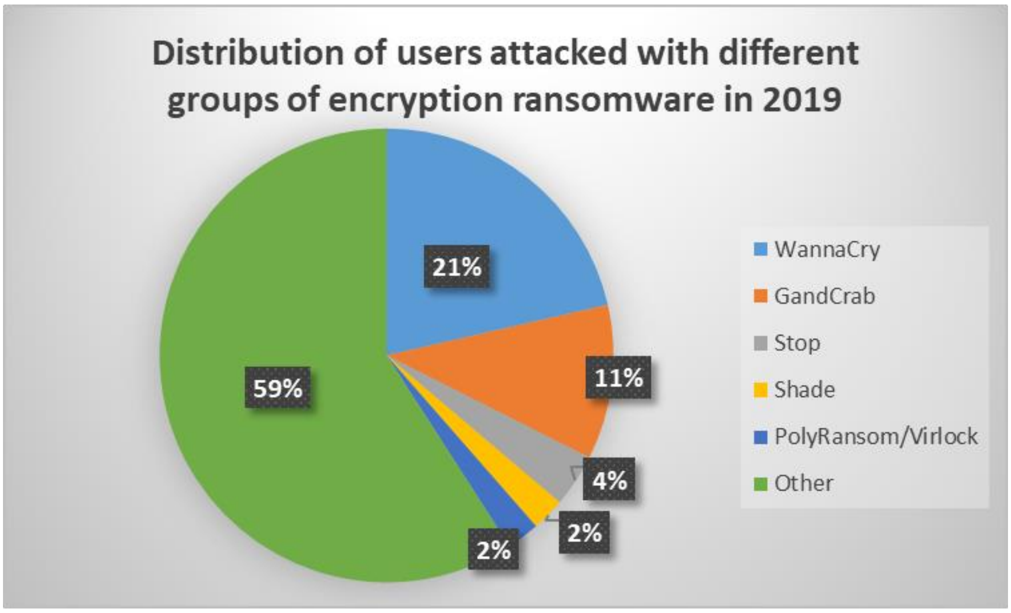
The most active ransomware families

Crypto-ransomware—malware that encrypts users' files until a ransom is paid—still makes up a significant portion of the total number of ransomware attacks: **48%** percent for the entire period from January 2018-March 2020: **46% in 2018, 49% in 2019, and 47% in 2020 Q1**.

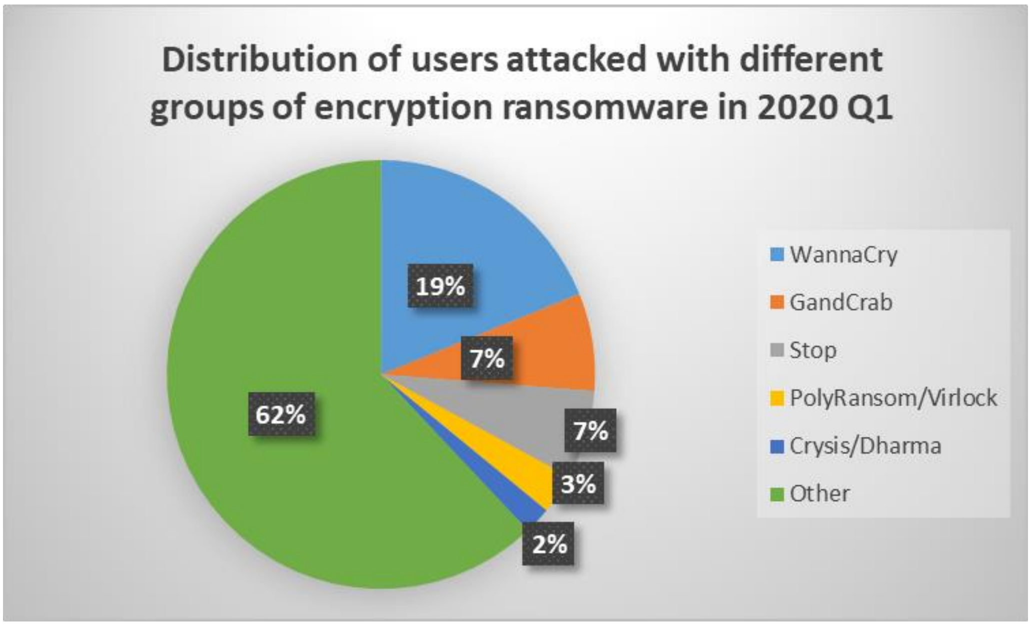
For 2018, WannaCry, the infamous encryptor that swept devices around the world in 2017, still remained active—affecting **34%** of all users that encountered crypto-ransomware attacks. One new ransomware family also entered the mix: GandCrab. This encryptor follows the ransomware-as-a-service model: the criminals sell their technology to the broader community. Other older ransomware families are also still clearly active: Shade, Cerber, and Cryakl.



In 2019, WannaCry once again impacted the highest number of Kaspersky users—only the percentage declined to **21%**; it attacked 164,433 users out of the 767,907 users that were attacked by encryptors. Shade and GandCrab remained active, but less so, and a new family entered the scene: Stop. This malware is spread through malicious installer bundles imitating software commonly searched for by users.



WannaCry attacks continued in 2020, as did those by GandCrab and Stop. The past years demonstrate a trend that was first noticed back in early 2018: the ransomware landscape has continued to consolidate, with only a few notable families maintaining a presence.



Geography

For 2018, the list of countries with the highest share of users attacked with ransomware was as follows:

Country	% of users attacked with ransomware out of all users encountering malware
Afghanistan	30.64%
Pakistan	20.99%
Iran	17.69%
Bangladesh	15.24%
Ethiopia	14.65%
Suriname	9.28%
Papua New Guinea	8.49%
Saint Lucia	8.33%
Somalia	8.11%
Uzbekistan	7.97%

The list of countries with the biggest share of users attacked with ransomware as a proportion of all users attacked with any kind of malware in 2018

The greatest percentage of ransomware attacks occurred primarily in the Middle East and Africa. It is possible that these regions are less protected against ransomware attacks, making them a more popular target for criminals. Both regions have complex political situations, meaning the attackers might see them as presenting an opportunity to encrypt and hold for ransom politically sensitive information.

For 2019, the countries with the highest share of users attacked with ransomware were similar to those from 2018:

Country	% of users attacked with ransomware out of all users encountering malware
Afghanistan	26.44%
Bangladesh	23.15%
Pakistan	19.07%
Iran	15.45%
Papua New Guinea	15.20%
Mozambique	12.02%
Turkmenistan	11.27%
Uzbekistan	10.50%
Ethiopia	8.59%
Tajikistan	8.08%

The list of countries with the biggest share of users attacked with ransomware as a proportion of all users attacked with any kind of malware in 2019

Once again, Africa and the Middle East were popular areas for ransomware activity. In addition, attackers began targeting Central Asian countries. Given that Central Asia is still a developing region, these countries may be seen as more vulnerable to ransomware by cyber criminals—and hence, a good target.

So far, for 2020, the countries with the highest share of users affected by ransomware are as follows:

Country	% of users attacked with ransomware out of all users encountering malware
Afghanistan	15.29%
Papua New Guinea	14.51%
Bangladesh	14.20%
Pakistan	13.63%
Solomon Islands	9.80%
Iran	9.29%
Virgin Islands	7.46%
Yemen	6.58%
Montenegro	6.18%

Turkmenistan	5.89%

The list of countries with the biggest share of users attacked with ransomware as a proportion of all users attacked with any kind of malware in 2020 Q1

Once again, despite a moderate decline in numbers, we can see considerably high levels of activity in the Middle East. The biggest takeaway from this is that ransomware is a truly ubiquitous threat—one should continue to track the activity of even those types of malware that seemingly disappeared.

Conclusions and predictions

Ransomware activity has continued to decline, but it still remains a prevalent threat. For example, WannaCry, the ransomware that reached epidemic levels in early 2017, infecting hundreds of thousands of computers worldwide, continues to spread due to its self-propagating properties. Heading into the first few months of 2020, it is still the most active type of crypto-ransomware. What's more, ransomware attacks are particularly destructive, frequently forcing operations to shut down—and often carrying a heavy financial toll. This is even truer now that ransomware attackers have shifted their focus from individuals to businesses: in 2019, **almost a third (30%)** of those targeted by ransomware were corporate users. WannaCry alone is estimated to have caused more than $4 billion in financial losses

When it comes to hospitals and other healthcare organizations, not only is confidential information and money at stake—but so are people's lives. Ransomware attacks disrupt the general operations of these organizations when their services are most needed. Of course, it is precisely because the healthcare sector is under increased pressure that it's being targeted—it's more vulnerable to attack. As the pandemic continues to unfold, it is likely the ransomware landscape will continue to evolve with it, with ransomware criminals looking for more ways to take advantage of the situation.

Actors behind mobile ransomware are targeting users worldwide, hitting even the smallest countries and most remote regions. This will most likely not change, meaning that all areas need to adopt appropriate security measures against these types of attacks. When it comes to specific crypto-ransomware families, only a few families will continue to maintain a presence. The rest of the attacks will come from newer and/or undefined actors. There will also be a shift from mass-scale ransomware campaigns (like WannaCry, which is no longer being developed by the creators) to targeted operations (like those facing the healthcare and energy industries). While the number of victims in these cases is small, they are carefully chosen by threat actors and often pose a much higher risk, with exorbitant ransoms requested.

Fighting back

The good news is that, as ransomware attacks continue, cybersecurity companies are able to develop tools to decrypt the infected files. Kaspersky recently released a decryptor for all strains of the infamous Shade ransomware. Dating back to 2015, the Shade ransomware encrypted office documents, pictures and archives and asked its victims to pay a ransom if they wanted them decrypted. Now, anyone who has been a victim of Shade can get their files back.

Kaspersky was also a co-founder of the No More Ransom initiative four years ago. The project offers various resources to help individuals and businesses recover their data and devices from ransomware attacks—including 52 free decryption tools.

On May 12, 2017, the largest ransomware epidemic in history—WannaCry—reached its peak. Today, it is still active, along with other ransomware families.

However, general security best practices, such as masking backups, updating software, and using protection tools should help organizations and individuals defend against the ransomware threat. Together with INTERPOL, Kaspersky encourages users to follow these practices to make May 12—**Anti-Ransomware Day**—free of ransomware

To prevent yourself from becoming a victim, Kaspersky experts, therefore, recommend:

1. Treat email attachments, or messages from people you don't know, with caution. If in doubt, don't open it.
2. Do not expose remote desktop services (such as RDP) to public networks unless absolutely necessary and always use strong passwords for them.
3. Back up data regularly. Make sure you can quickly access it in an emergency when needed.
4. Always keep software updated on all the devices you use. To prevent ransomware from exploiting vulnerabilities, use tools that can automatically detect vulnerabilities and download and install patches.
5. For personal devices, use a reliable security solution like Kaspersky Security Cloud that protects against file-encrypting malware and rolls back the changes made by malicious applications.
6. 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 from ransomware attacks is available here.
7. If you're a business, enhance your protection with Kaspersky's free **Anti-Ransomware Tool for Business**. Its recently updated version contains an exploit prevention feature to prevent ransomware and other threats from exploiting vulnerabilities in software and applications. It is also helpful for customers that use Windows 7: with the end of support for Windows 7, new vulnerabilities in this system won't be patched by the developer.
8. For superior protection, use an endpoint security solution, such as Kaspersky Endpoint Security for Business that is powered by exploit prevention, behavior detection and a remediation engine that is able to roll back malicious actions.
9. Carry out regular security audits of your corporate network for anomalies.
10. Don't overlook less obvious targets, such as queue management systems, POS terminals, and even vending machines, and ensure that you use a security solution designed for embedded systems

Last, but not least, remember that ransomware is a criminal offence. You shouldn't pay. If you become a victim, report it to your local law enforcement agency.