Digital Education: The cyberrisks of the online classroom

kaspersky

Contents

Foreword

Ilya Zalessky, head of educational services at Yandex

How the COVID-19 pandemic will affect the development of online education

While everyone's attention has been drawn to distance learning lately, the idea is not new, and the first correspondence schools appeared in the eighteenth century. The spread of this type of education has always been linked primarily to the development of various new means of communication.

So far, there have been three types of distance learning. First, traditional offline education, in which most of the interactions between the student and the teacher take place in person, and homework performs the role of the remote component. Second, mixed learning, when some of the classes and other activities take place online, but students still have to attend school. Finally, full distance education, which used to be very rare in schools.

It was assumed that the elements of online education would gradually fit into the ordinary educational process. However, the pandemic has forced everyone to move from offline schooling to the world of completely remote education, doing so instantly and with no preparation. This led to most schoolteachers being forced to adapt, under extreme conditions, to teaching online.

Prior to self-isolation, sixty percent of Russian schools did not use distance learning at all, and only twenty percent of teachers had experience using resources and technologies for remote teaching. Students were also unfamiliar with the format: by the beginning of the academic year 2019/2020, only four to six percent of Russian schoolchildren had used online education.

We managed to sustain the continuity of the academic process thanks to two factors. **The first one is a well-developed online education ecosystem in Russia and healthy competition among different educational platforms.** The pandemic has been a real test for all digital educational resources, none of which, public or private, were designed to deal with such explosive growth in traffic. Yet the variety of platforms and tools and coordinated steps by market players have allowed everyone to continue their studies.

The second factor is teachers' dedication. In the initial stages of distant education, they had to improvise and adjust the processes on the go. There has been criticism of both online tools and outdated learning approaches that were not applicable to the entire distance education process, but eventually, teachers were able to ensure that the educational process was comfortable and productive.

After such an explosive spread of distance education, it was important for us to get feedback from teachers. Here is what the study by the Yandex team showed:

- **Teachers combine digital and non-digital tools.** Although 97% of respondents used digital tools (such as video tutorials and automatic job verification systems), many of them still gave additional tasks from traditional textbooks or sent out printed materials.

- **Teacher experience has little impact on the use of online tools.** Teachers with different backgrounds can use online practices equally well.

- **Teachers' workload has increased, even though the number of assignments has remained the same.** The amount of homework that students receive, on average, has not changed. But the workload of teachers has increased. One of the key reasons is an increase in communications with parents.

- **In primary school,** diagnostics and control have been affected more seriously, and in middle and high school, review of materials and practice have suffered the most.

- **Video conferences are not a silver bullet.** Only 32% of surveyed teachers regularly conduct video lessons. Perhaps this is linked to the fact that the tradition of online control and proctoring in schools is not developed as well as in universities.

- **The most common remote work tools are printed materials and automatic verification platforms.** They are suitable for all pedagogical purposes, and they have been used by 88% of teachers.

It is already clear that this recent experience of using distance education tools may become useful earlier than expected. In autumn, children will return to schools, and even if a full-on second wave of the pandemic does not happen, difficulties may arise locally when pupils with even a slight cold are made to study from home. And in cases of infection, part of students or schools within the same district may drop out of the usual offline educational process.

In addition, teachers familiarized themselves with various online services and tools, and were able to build their own approaches to mixed learning. Over the summer, they had the opportunity to reflect on what digital tools they may want to use in normal work. So, the demand for digital tools is likely to continue to grow.

The popularity of these tools may also increase due to the fact that some schoolchildren enjoyed distance education. According to a survey by the Foundation of National Educational Resources, almost a quarter of

schoolchildren would like to continue distance learning after the pandemic, and 21% see new opportunities in this model of studying. For 40%, video lessons were more comfortable psychologically than face-to-face classes. It is important to pay close attention to these students. Perhaps they make up a majority of those who will leave school and attend external training to prepare for state exams in higher education institutions.

To conclude, the key outcome of remote education is an increase in digital literacy, both for children and teachers. This means that the forms of the learning process should become more diverse, meet modern needs, and take advantage of new technological opportunities. The growing popularity of digital services in education will also contribute to the demand for cybersecurity. After working with distance learning, teachers, principals and parents were able to realize the importance of digital security, and it turned from an abstract notion into a necessity for maintaining a normal learning process. It is now up to the industry to introduce digital security lessons for teachers, so that they can pass on new knowledge and skills to their students.

Insights from the Classroom:

Steven Furnell, professor of cybersecurity, University of Nottingham

Reflections on digital education delivery during the COVID-19 pandemic

I was involved in a variety of student-facing activities during lockdown, including delivery of lectures, supervision and assessment of projects, and supervision of work placements. All of these would normally have occurred face-to-face, and I felt that things adapted pretty quickly, without fundamentally changing the nature and quality of what we were able to achieve. Of course, some subject areas have the potential to feel a more pronounced impact than others, and to some extent, the computing-based topics that I am involved with are shielded from some of the more significant impacts because it is easier to replicate (or allow remote access) to the necessary resources. The same would not be true for courses in which the student experience is tied to things like the use of other types of specialist laboratories and facilities, or the ability to conduct fieldwork.

Even in the subjects where the main delivery could continue fairly easily, it was not simply a case of "flipping a switch" to move over to digital delivery. Certain forms of assessment needed to change – most notably closed-book examinations and tests – but overall, it was perhaps something of an object lesson in how quickly and easily things could change in terms of the mode of delivery, without fundamentally compromising the content and learning outcomes of the course. I think it certainly opened more peoples' eyes to the potential for things to be delivered more flexibly moving forward.

In terms of the students' opinions, I'd say they were generally happy and felt able to work (and some actively preferred the more flexible approach). I think what was more problematic for some of them was the wider isolation of the lockdown context, and the effect that this had on their mood or mental health (which of course had the potential to affect their ability to study). Ultimately, it certainly was not the sort of "university experience" they had signed up for, but they were equally pragmatic in understanding that the situation was not of anyone's making and that credible efforts were being made to ensure that things could continue as effectively as possible.

I know that many universities also took explicit steps to ensure that students were not disadvantaged in terms of grades (e.g. calculating the result for the year based on the best n credits rather than the full year of results, to offset impacts that may have been caused by the disruption). As such, I think students were also able to take reassurance from this and focus on completing their studies for the year without continual concern that COVID-19 was going to undermine their efforts.

At the same time, it was not all smooth sailing, because the change being forced upon them unexpectedly shone a light on the fact that some students (and indeed some staff working from home) did not live in areas with good broadband access, or they lacked the necessary devices to work/study comfortably from home and so certain provisions needed to be made for them.

It is easy to imagine that if digital delivery were able to be approached in a more planned manner – as indeed many universities have now done in preparation for the next academic year – then it will be able to form part of a more integrated academic experience. In fact, looking beyond COVID-19 as the driver, it will be interesting to see how many more universities will then use their newfound experience as a basis to enable more flexible delivery by default. It certainly does not mean the abandonment of traditional aspects, such as lectures and physical attendance, but it does help to show how things can be adapted and delivered more flexibly to enable work-based and part-time study and to increase the overall accessibility of the university experience to those who might not otherwise be able to take part.

Of course, alongside this positive outlook, we should not forget that the increased use of technology brings considerations from a cybersecurity perspective. Universities themselves immediately become more dependent upon their technology infrastructure, such that any resultant attacks and breaches can have an even more profound impact upon their operations. In addition, there is the potential for the digital delivery technologies to be directly targeted, and we have already seen the evidence of such attacks, such as vulnerability exploitation, phishing and denial of service being specifically directed towards online learners and providers.

There is also the more general potential for users to be less protected than they would normally be within the campus environment, unless the university has made specific provisions to support and guide them (in relation to both technology and awareness). Obviously, many students use their own devices on campus anyway, but the main university-provided systems that they rely upon in labs and open access areas are still centrally managed and monitored. Outside of this environment, they are left potentially more exposed, operating from devices and networks that may not be securely configured and without the on-site support that they might normally turn to. This is not to say that provisions cannot be made to help them, but it needs to be factored into the changes, alongside the academic delivery. As such, it is important to recognize that a transition to digital delivery will mean a change for supporting services, such as the cybersecurity team and the help desk, just as much as it will for the academics and the students.

Distance Learning

This past spring, as the COVID-19 pandemic took hold, online learning became the new norm as universities and classrooms around the world were forced to close their doors. By April 29, 2020, more than 1.2 billion children across 186 countries were impacted by school closures.

Shortly after schools began to transition to emergency remote learning, it became clear that many were not ready for the kind of full-time, digital education now needed. Not all students had the technology that was required, from laptops to a stable Internet connection, and parents and instructors in countries like the United States worried students would inevitably fall behind academically. What is more, many educational institutions did not have proper cybersecurity measures in place, putting online classrooms at increased risks of cyberattacks.

In fact, in June, Microsoft Security Intelligence reported that the education industry accounted for 61 percent of the 7.7 million malware encounters experienced by enterprises in the previous 30 days – more than any other sector.

Apart from malware, educational institutions were also at increased risk of data breaches and violations of student privacy. It was this spring that "Zoombombing" became part of the general lexicon after pranksters and ill-intentioned individuals began taking advantage of Zoom's security weaknesses to break into private meetings. Among the victims were schools, with several reported incidents of online classrooms being interrupted by users making lewd comments or streaming pornography.

As fall approaches, digital learning will continue to be a necessity. In fact, half of all U.S. elementary and high school students will be entirely online. Even those institutions that are reopening are deploying some kind of hybrid model, such as delivering large lectures online. What's more, the threat of a second coronavirus wave still remains, meaning that future large-scale school closures are still a possibility.

With this in mind, Kaspersky researchers took a closer look at the cyber risks faced by schools and universities, so that educators can be prepared moving forward – and take the necessary precautions to stay secure.

Methodology

This report examines several different types of threats – phishing pages and emails related to online learning platforms and video conferencing applications, threats disguised under the names of these same applications, and distributed denial of service (DDoS) attacks affecting the education industry.

Various threats disguised under popular online learning platforms/video conferencing applications

For this part, we utilized results from the Kaspersky Security Network (KSN) – a system for processing anonymous data related to cybersecurity threats shared voluntarily from Kaspersky users – for two different periods: January-June 2019 and January-June 2020.

Using KSN, we searched for files bundled with various threats that contained the name of one of the following platforms/applications during one of the two periods above:

1) Moodle – the most popular learning management system (LMS) in the world. It s used by educators to build online courses, host classes and create activities.

2) Blackboard – another popular LMS. It provides a virtual learning environment where educators can build entirely digital courses or create additional activities to supplement in-person instruction.

3) Zoom – a highly popular online collaboration tool that provides free video conferencing capabilities. Many educators used Zoom to conduct online classes this past spring.

4) Google Classroom – a web service designed specifically for educators to host classes, generate assignments and track students' progress.

5) Coursera – a popular online learning platform that hosts a variety of open online courses, certificates and even degree programs.

6) edX – a provider of open online courses available to users worldwide.

7) Google Meet – a video communication service similar to Zoom, which can be used to host meetings and online classes

The results display those (PC and mobile) users that encountered various threats disguised as the above platforms/applications from January-June 2019 and January-June 2020.

Distributed denial of service (DDoS) attacks

Kaspersky tracks DDoS (distributed denial of service) attacks using the Kaspersky DDoS Intelligence System. A part of Kaspersky DDoS Protection, the system intercepts and analyzes commands received by bots from C&C servers. The system is proactive, not reactive, meaning that it does not wait for the user's device to get infected or a command to be executed. Each "unique target" represents a specific IP address that was attacked.

The following report displays the percentage of DDoS attacks that affected educational resources out of the total number of DDoS attacks registered by the Kaspersky DDoS Intelligence System for Q1 2019 and Q1 2020.

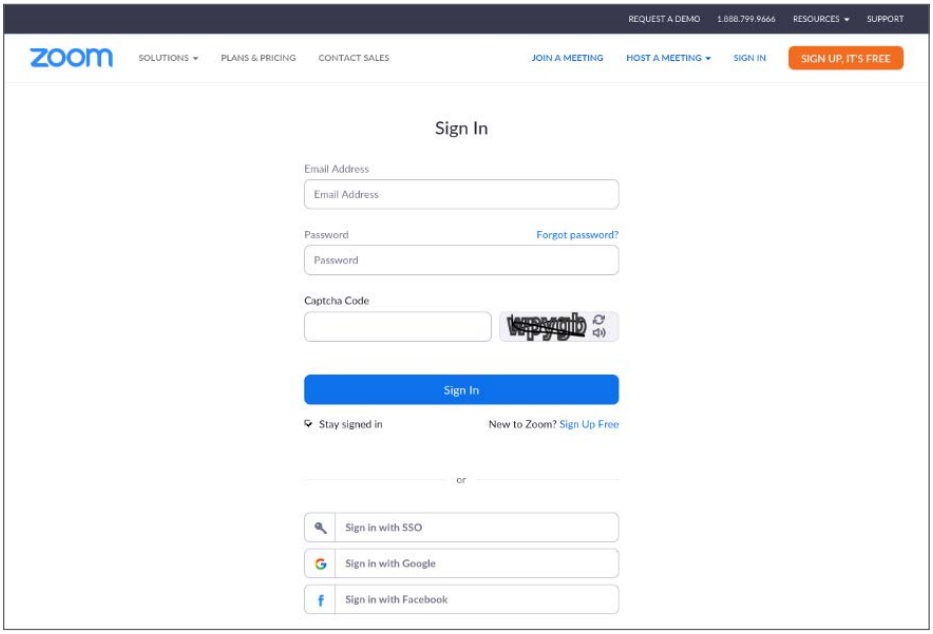
Our Key Findings

- The number of DDoS attacks affecting educational resources grew by **550%** in January 2020 when compared to January 2019.
- For each month from February to June, the number of DDoS attacks that affected educational resources out of the total number of attacks was **350-500%** greater in 2020 than in the corresponding month in 2019.
- From January to June 2020, the total number of unique users that encountered various threats distributed under the guise of popular online learning platforms/video conferencing applications was **168,550 – a 20,455% increase** when compared to the same period for 2019.
- From January to June 2020, the platform most commonly used as a lure was Zoom, with **99.5%** of the users that encountered various threats encountering them via files that contained the name Zoom. The second most common platform used as a lure was **Moodle**.
- By far the most common threats encountered in 2020 were downloaders and adware, which were encountered in **98.77%** of the total registered infection attempts. Various classes of trojans were the second most common.
- For threats distributed under the guise of popular platforms for conducting online classes in 2020, the greatest number of infection attempts registered came from Russia (**71.21%**) followed by Germany (**21.25**).

kaspersky

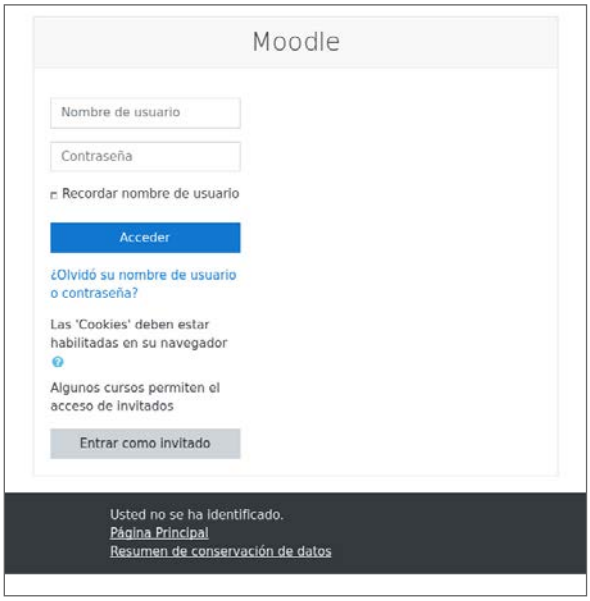
Phishing risks of online learning platforms / video conferencing applications

It is not unexpected that phishing, one of the oldest and most popular forms of cybercrime, would reach educational organizations. In fact, a host of phishing websites for popular platforms like Google Classroom and Zoom began to pop up following the switch to distance learning. From the end of April to mid-June, Check Point Research discovered that 2,449 domains related to Zoom had been registered, 32 of which were malicious and 320 of which were "suspicious". Suspicious domains were also registered for Microsoft Teams and Google Meet. Users who land on these phishing pages are often tricked into clicking URLs that download malicious programs, or they might be tricked into inputting their login credentials, which would put these in the hands of the cybercriminals.



Fake login page for Zoom

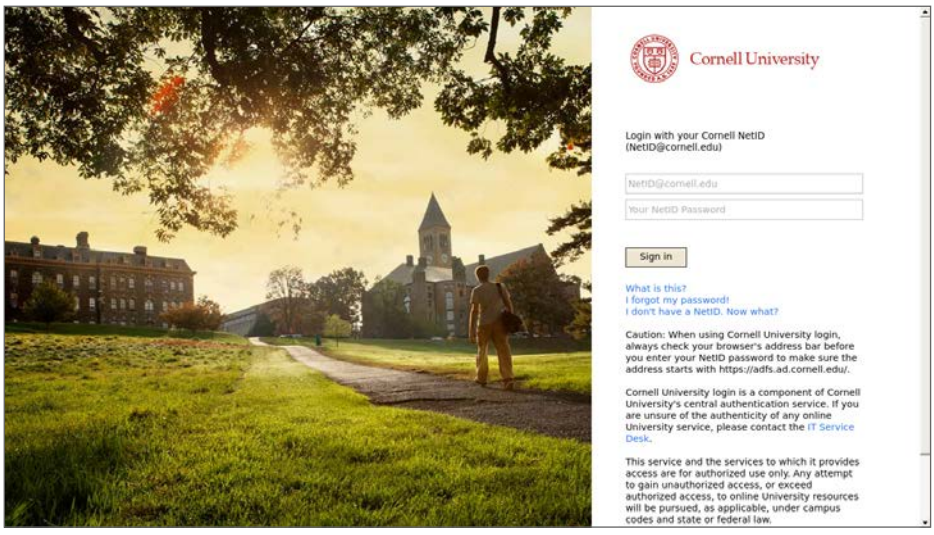
kaspersky



Fake login page for Moodle

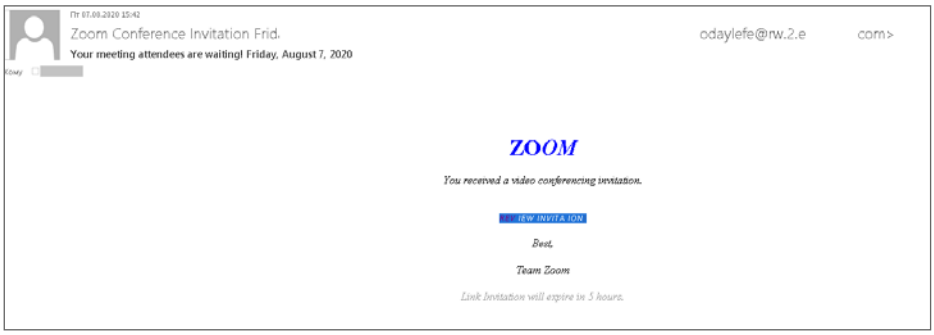
These criminals might not even be after access to your account. They can use your login credentials for various nefarious purposes: launching spam or phishing attacks, gaining access to your other accounts as people often reuse passwords, or collecting more personally identifiable information to be used in future attacks / attempts to steal funds.

Most universities also have their own platforms where students and faculty can login to access important resources and various academic services. This past spring, some attackers went so far as to target specific universities by creating phishing pages for their individual academic login pages.



Phishing page for Cornell University's academic login page

Apart from fake web pages, cybercriminals sent out an increasing number of phishing emails related to these same platforms. These told users they had missed a meeting, a class had been canceled, or it was time to activate their accounts. Of course, if they opened the email and clicked on any links, they were at risk of downloading various threats.



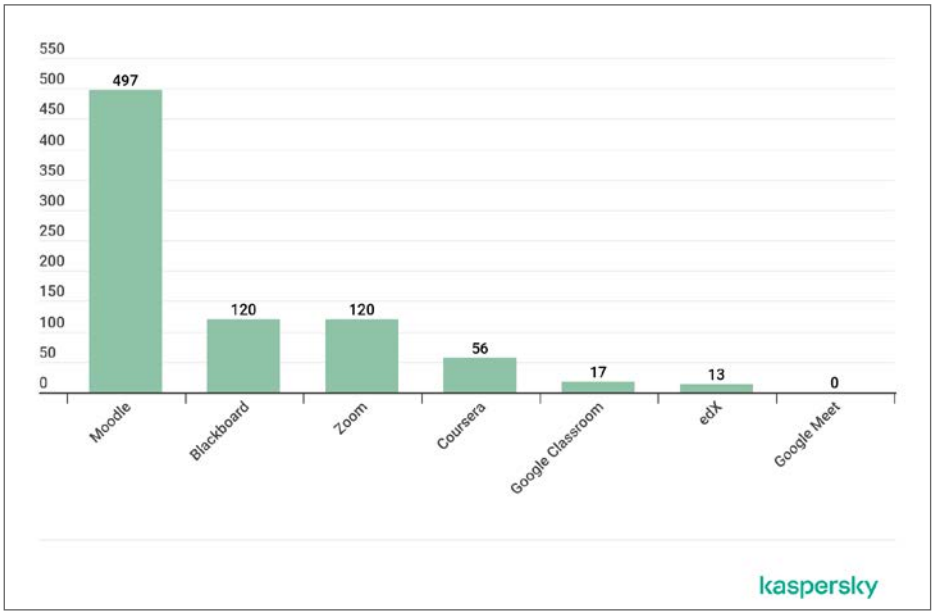
Phishing email supposedly from Zoom urging the user to review a new video conferencing invitation

The cyberthreats of online learning platforms

A common way to distribute threats disguised as popular video meeting apps and online course platforms is by bundling threats as legitimate application installers.

There are several ways users can encounter these malicious installers. One way is through phishing websites designed to look like the legitimate platforms, as seen above. Those users who inadvertently end up on the wrong page are then exposed to malware or adware when they attempt to download what they believe is the genuine application. Another common way is through phishing emails disguised as special offers or notifications from the platform. If users click the links in the email, then they are at risk of downloading unwanted files.

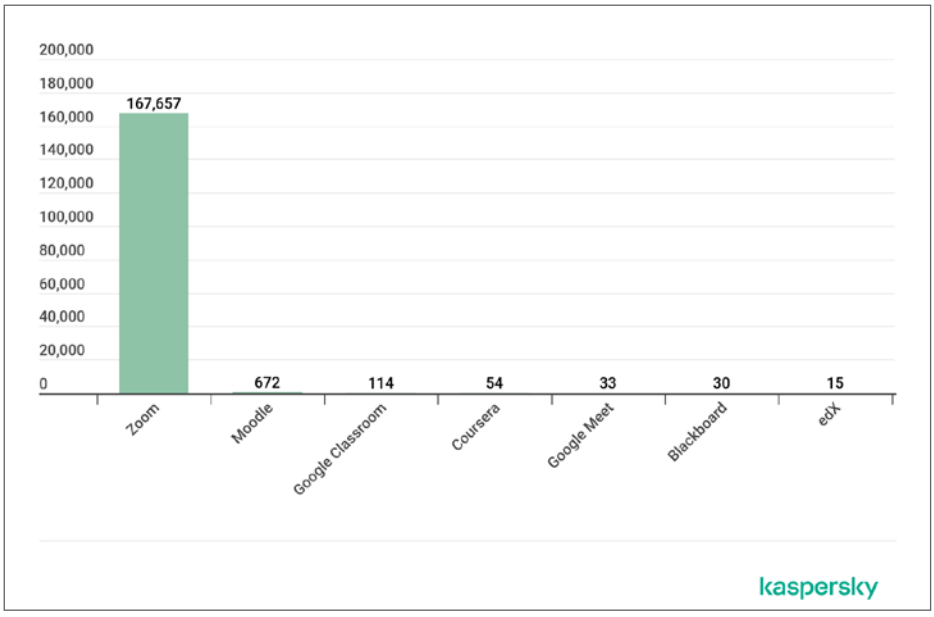
From January to June 2019, the number of unique users that encountered various threats distributed via the platforms specified in the methodology section of this report was **820**.



The number of unique users that encountered various threats disguised as popular online learning/video conferencing platforms, January – June 2019

The most popular lure was Moodle, with Blackboard and Zoom being the second most popular.

In 2020, however, the total number of users that encountered various threats disguised as popular online learning platforms jumped to **168,550, a 20,455% increase**.



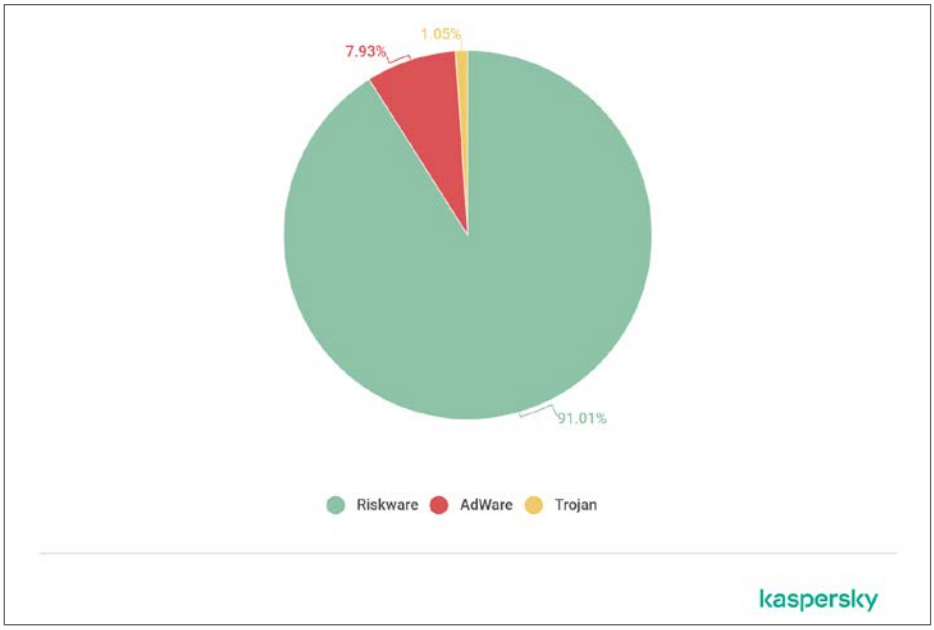
The number of unique users that encountered various threats disguised as popular online learning/video conferencing platforms, January – June 2020

kaspersky

Zoom was far and away the platform most frequently used as a lure, with **99.5%** of users encountering various threats disguised under its name. This is not surprising given that Zoom became the go-to video conferencing platform. By February 2020, the platform had added more new users (2.22 million) than it had in all of 2019 (1.99 million). As of April 30, the company claimed to have 300 million daily meeting participants. Given its immense popularity, it is only logical that it would be the preferred target for malicious actors. And, with millions of more users looking to download the application, the chances are high that at least some of these would come across fake installers or setup files.

A closer look at the 2020 threat landscape

Types of threats encountered



Percent distribution of different types of threats disguised as popular online learning / video conferencing platforms encountered by users, January - June 2020

By far the most common threats distributed under the guise of legitimate video conferencing/online learning platforms were not-a-virus (**99%**). Not-a-virus files are typically divided into two categories: riskware and adware. Adware bombards users with unwanted ads, while riskware consists of various files – from browser bars and download managers, to remote administration tools – that may carry out various actions on your computer without your consent.

About **1%** of the infection attempts were various trojan families: malicious files that allow cybercriminals to do everything from deleting and blocking data to interrupting the performance of the computer. Some trojans encountered were password stealers, which are designed to steal your credentials, while others were droppers and downloaders, both of which can deliver further malicious programs on your device.

Other threats encountered were backdoors, which allow the attackers to take remote control over the device and perform any number of tasks; exploits, which take advantage of a vulnerability in an operating system or application to gain unauthorized access to/use of the latter; and DangerousObjects (non-specific malicious files).

A regional perspective

The five countries where the greatest number of infection attempts were registered are as follows:

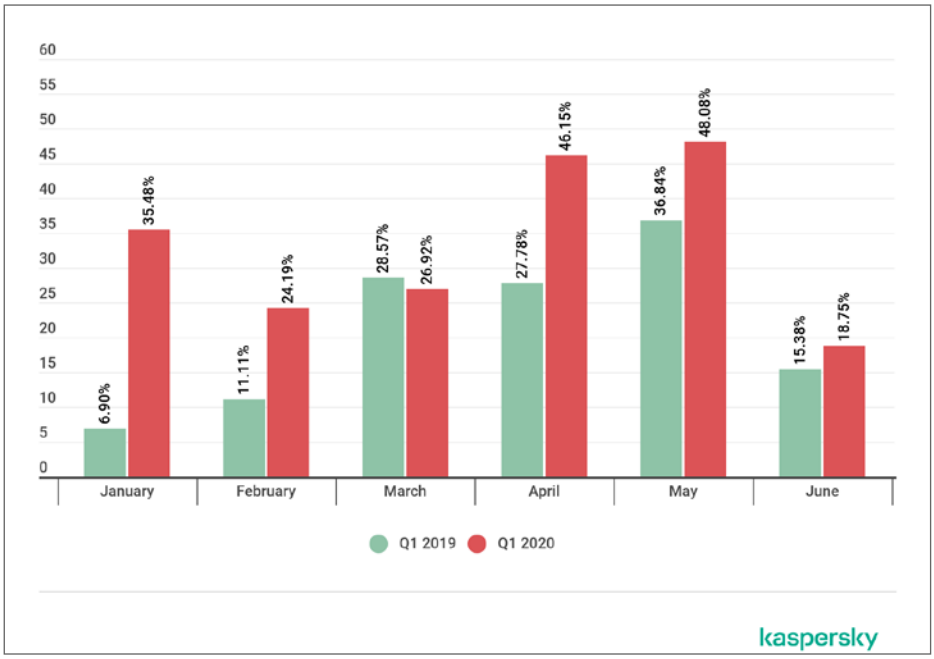
Russia	70.94%
Germany	21.25%
Austria	1.44%
Italy	1%
Brazil	1%

For threats distributed under the guise of popular online learning / video conferencing platforms, the greatest number of attempts to infect users occurred in Russia (**70.94%**). The second greatest number came from Germany (**21.25%**). Both countries closed schools early in mid-March, making remote learning the only option for millions of teachers and students. In addition, video conferencing has become incredibly popular in Germany, with more than half of Germans regularly using it as a tool for work or school. Given the overall global popularity of Zoom, a significant portion of Germans most likely use this platform and – given that Zoom is by far the most popular platform used as a lure – encountered various threats as a result.

Educational resources hit by DDoS attacks

In April, a large Turkish university was forced entirely offline for 40 minutes after it was hit with a DDoS attack on the morning of exams. In June, a major university in the northeastern United States had its exams disrupted after a DDoS attack affected its online test platforms. These are just two examples of a larger trend that began after schools were forced to transition to emergency remote learning: the rise of DDoS attacks against the education sector.

In general, the total number of DDoS attacks increased globally by 80% for Q1 2020 when compared to Q1 2019. And a large portion of that increase can be attributed to the growing number of attacks against distance e-learning services.



Percent of the total number of DDoS attacks that affected educational resources: Q1 2019 vs Q1 2020

When compared to Q1 2019, the percentage of DDoS attacks affecting educational resources out of all DDoS attacks increased steadily for each month of Q2 2020 (with the exception of March). When looking at the total number of DDoS attacks that occurred between January and June 2020, the number of DDoS attacks affecting educational resources increased by at least 350% when compared to the corresponding month in 2019.

Percent increase when compared to 2019	January: 550%	February: 500%	March: 350%	April: 480%	May: 357.14%	June: 450%

The percent growth in the number of attacks on educational resources when compared to the same month of the previous year

The more educational organizations rely on online resources to conduct their regular activities, the more of a target these networks become for cybercriminals looking to disrupt their operations.

Looking forward

Online learning is not a short-term response to a global pandemic. It is here to stay.

For one, the pandemic is not over. Many students are still studying virtually, at least part of the time, and some schools that decided to open have already decided to revert back to online classes only. The possibility of a second wave still looms, meaning educators have to be prepared for large-scale school closures in the future.

Even when the pandemic does end, most agree that online learning will not disappear altogether. A recent global survey by Pearson Education, an academic publishing company, found that nearly 90% of the 7,000 individuals surveyed expect online learning to continue to play a role at all education levels.

In fact, even before the pandemic, some universities had already developed blending curricula (a mix of offline experiences and online courses). More and more academic institutions are considering this as an option for future programs.

However, as long as online learning continues to grow in popularity, cybercriminals will attempt to exploit this fact for their own gain. That means educational organizations will continue to face a growing number of cyber risks – into this fall and beyond. Fortunately, engaging – and secure – online academic experiences are possible. Educational institutions just need to review their cybersecurity programs and adopt appropriate measures to better secure their online learning environments and resources.

To get started, here are a few ways to protect your organization against cyber risks:

To stay safe from phishing:

- Do not visit websites until you are sure they are legitimate and start with "https".
- Once on a website, check that it is authentic.
  - Double-check the format of the URL or the spelling of the company name, as well as read reviews and check the domain's registration data before starting any downloads.
- For emails, look carefully at the sender's address: if it comes from a free email service or contains meaningless characters, it is most likely fake.
- Pay attention to the text: well-known companies would not send emails with poor formatting or poor grammar.

- Do not open attachments or click links in emails from these platforms, particularly if the sender insists upon it. It is better to go to the official website or app directly and log into your account from there.
- Use a reliable security solution like Kaspersky Security Cloud that identifies malicious attachments and blocks phishing sites.

To stay safe from malware and other threats disguised as video conferencing apps / online learning platforms:

- Do not download any unofficial versions or modifications of these applications/platforms.
- Use different, strong passwords for each of your accounts.
- Always make sure you are on the official company website before proceeding to download anything to your device.
- Use a reliable security solution like Kaspersky Security Cloud that delivers advanced protection on all your devices.

To stay safe from DDoS attacks:

- Maintain web resources operations by assigning specialists who understand how to respond to DDoS attacks. They must also be prepared to respond out of hours, during evenings and weekends.
- Validate third-party agreements and contact information including those made with internet service providers. This helps teams quickly access agreements in case of an attack.
- Implementing professional solutions will safeguard an organization from DDoS attacks. For example, Kaspersky DDoS Protection combines Kaspersky's extensive expertise in combating cyberthreats and the company's unique in-house products.

Afterword: What the future might hold

Dr. Michael Littger, executive director, Deutschland sicher im Netz e.V. (NGO promoting greater IT security in Germany)

The Digital Future of Education

The end of the last school year was a tumultuous one not only for many pupils, students and teachers, but also for parents and families. While a remarkable number of schools and teachers came up with new and creative ideas to use the lockdown for advancing digital teaching, far too many schools in Germany are still underequipped for providing safe and adequate online education to their students. Overall, the Corona pandemic has thrown into sharp focus the need for more digital education.

The German National Education Report (Nationaler Bildungsbericht), which was published in the summer of 2020, shows that more than 95% of students between twelve and nineteen own a smartphone, which they also use for school. At the same time, more than a third of students say that exciting and engaging digital teaching is the exception in their classrooms. About one in six says that digital topics do not play a role in their classrooms at all.

One of the key reasons for this is a lack of infrastructure and technical equipment that many schools in Germany are facing, the report concludes. The DigitalPakt Schule ("digital pact for schools"), which was finalized in March 2019, aims to provide all schools in the country with adequate equipment, including computers, laptops, tablets, wireless Internet access and similar amenities. While these investments are an important and necessary step, they can only be a starting point for the digital future of education.

Enabling teachers to become drivers of digital education

It should not be overlooked that new hardware and software in schools can only be used effectively if educators know how to do so safely and adequately in the classroom. As the National Education Report notes, digital education means a lot more than simply reusing traditional offline learning materials in an online setting. The success of digital teaching depends on teachers' ability to reflect digital media didactically and discuss their use and application critically with students. Yet in general, teachers' confidence in their ability to utilize digital tools effectively and creatively in the classroom remains low.

Furthermore, educators have information security and data protection factors to consider. How can the digital classroom be held in a secure environment? How can data security be guaranteed? Which tools and software are

admissible? For most teachers, these and related topics have never been part of their own curriculum. In a digital classroom, however, media literacy, data protection, and digital didactics are key to creating a safe and inclusive digital learning space for all students. So, where do schools and teachers start?

Shaping the present and future of digital teaching

The project DigiBitS was established in 2016 by Deutschland sicher im Netz e.V. (DsiN) to support schools and teachers in facilitating digital education at their institutions. Since its foundation, the project has been joined by more than 200 schools across Germany and provided practical tools for implementing digital teaching in everyday classes.

Three main fields of action have emerged, where schools and teaching staff can be actively supported in implementing digital education. They form the core of the DigiBitS-program for the academic year 2020/2021 and can be applied to support structures in digital education more broadly:

1. **Acquisition: Training teachers to become digital role models**
   DigiBitS has developed a program that includes online and offline training sessions, networking meetings and seminars. They are designed to highlight various topics, methods and tools needed for teaching in a digital setting.

2. **Teaching: Learning how to prepare a class digitally**
   In many cases, teachers still lack resources and materials to implement digital teaching in their classrooms. DigiBitS provides lesson plans, checklists and tool tips as a means of integrating digital topics and tools more efficiently.

3. **Networking: Sharing knowledge and best practice**
   Creating a nationwide network of partner schools and cooperation partners from across the field of digital education facilitates discourse and the sharing of learning. Through intense cooperation, teachers and schools develop their own guidelines and standards on how to instruct digitally in a safe manner.

Digital education is a herculean challenge that concerns not only policymakers, educators, and students, but all parts of society, which stand to gain from the advancements made in digital teaching. Countless initiatives and projects such as DigiBitS have shown the need to equip and inspire teachers to use digital possibilities in the classroom while also providing them with the necessary infrastructure to create compelling digital classes that reach and engage all students. These insights must now be implemented into structures that work for schools and educational institutions everywhere.