# Cybersecurity threatscape

## Q4 2020

ptsecurity.com

# Contents

# Executive summary

Highlights of Q4 2020 include:

- The number of incidents grew by 3.1 percent compared to the previous quarter. The share of hacking as an attack method on organizations continues to increase, from 30 percent in Q3 to 36 percent in Q4. In incidents affecting individuals, on the contrary, experts recorded a surge in the use of social engineering: 67 percent in Q3 versus 85 percent in Q4.
- Throughout the year, we saw steady growth in ransomware attacks, and Q4 was no exception. Ransomware accounted for 56 percent of all malware attacks (compared to 51% in Q3). Among victims in our dataset, Ryuk ransomware was the primary culprit.
- For two years, industrial companies have been one of the three most tempting targets for attackers. Such attacks tend to be the handiwork of ransomware operators and APT groups. The RTM group has been particularly active: the PT Expert Security Center recorded 61 phishing attacks, with industrial companies among the targets.
- Clients of software vendor SolarWinds were affected by a high-profile supply chain attack. The incident affected over 40 organizations that had installed a compromised update of the SolarWinds Orion infrastructure monitoring platform. The hackers managed to steal penetration testing tools from security firm FireEye. These tools will likely resurface in future attacks for years to come.
- There was a spike in attacks on retailers and commerce. The number of attacks increased by 56 percent compared to Q3. Such a sharp increase is the work of ransomware operators and web skimmers placed by attackers on hacked store websites.
- In the late 2019, we shared our forecasts about how the threat landscape would change in 2020. We expected high-profile cyberattacks in the lead-up to the U.S. presidential elections. Our forecasts came true. Attackers hacked election support systems, stole money from parties' accounts, and sent numerous phishing emails on election-related topics. During the most recent election cycle, the Wisconsin Democratic Party caught over 800 phishing attempts.
- 40 percent of phishing campaigns leveraged interest in COVID-19 vaccines. The popularity of COVID-19 as a topic for social engineering remains unchanged from Q3 (4.6%). Despite the huge amount of news and other content on COVID-19, attackers still manage to strike the right note as they trick victims into entering credentials on fake websites, opening malicious attachments, or revealing their payment card data to send money to "people in need" or "pay for the vaccine."

To protect from cyberattacks, we recommend following our recommendations for personal and corporate cybersecurity. In light of recent attacks aimed at exploiting vulnerabilities in IT infrastructure, we urge companies to install patches without delay. To make it easier to identify and eliminate security flaws, companies should adopt an automated vulnerability management process. Companies should also deploy modern security tools, including web application firewall, network traffic analysis, and SIEM. To prevent attacks related to delivery of malware by email, we recommend checking attachments in a sandbox, a special virtual environment designed for analyzing file behavior.

# Statistics

Hacking as an attack method against organizations was already increasing in Q3 and continued climbing in Q4. From October to December 2020, the increase was 6 percentage points. Eight out of ten attacks were targeted. There was a surge in social engineering in attacks on individuals, from 67 percent to 85 percent.

The most common motive behind cyberattacks in Q4 2020 was data theft. Personal data and trade secrets are still of great demand in attacks on organizations. In attacks against individuals, hackers most often target credentials and personal data. Compared to the previous quarter, the number of incidents rose by 3.1 percent; compared to the same quarter last year, it was 41.2 percent larger.

***3.1% more cyber-attacks than in Q3 2020***

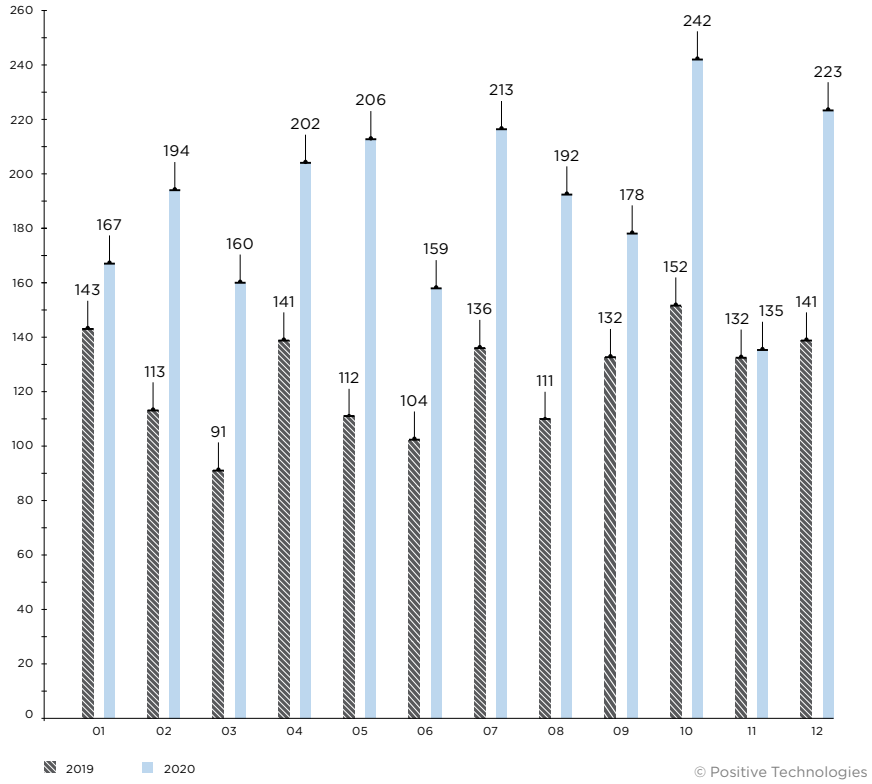


*Figure 1. Number of incidents per month in 2019 and 2020 (1 = January, 12 = December)*

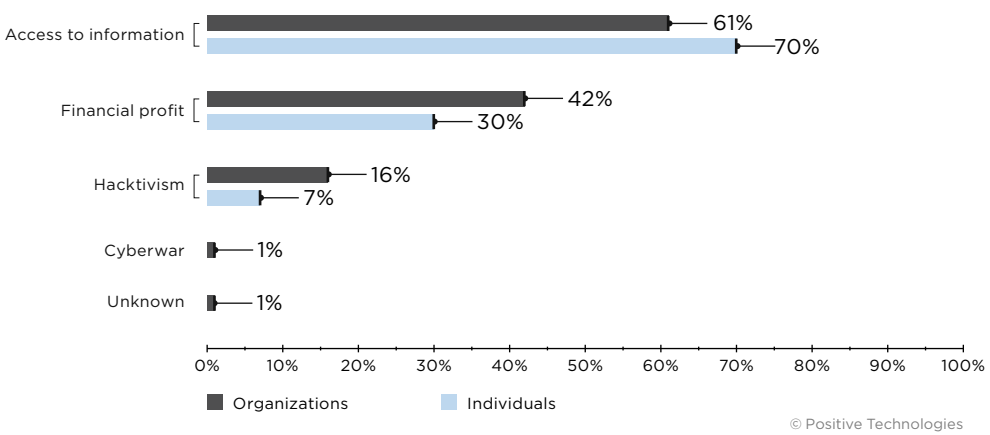


*Figure 2. Attackers' motives (percentage of attacks)*

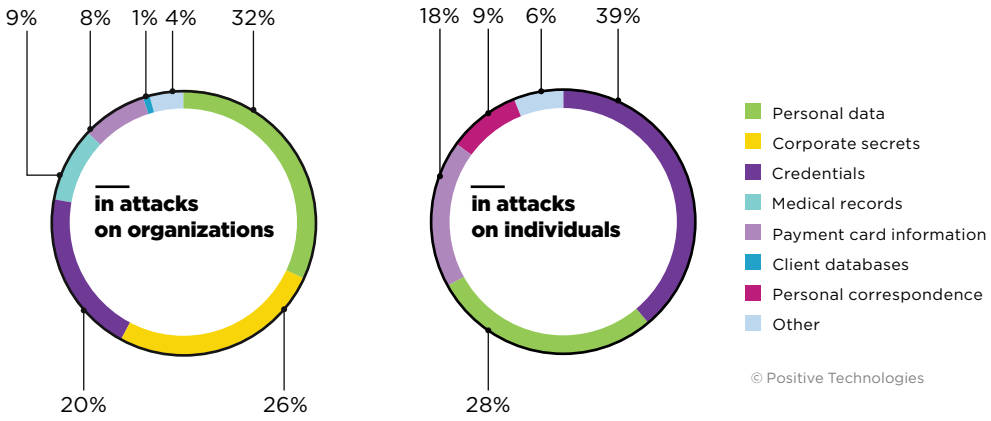


*Figure 3. Types of data stolen*

***80% of attacks are targeted***

***12% of attacks are directed at individuals***

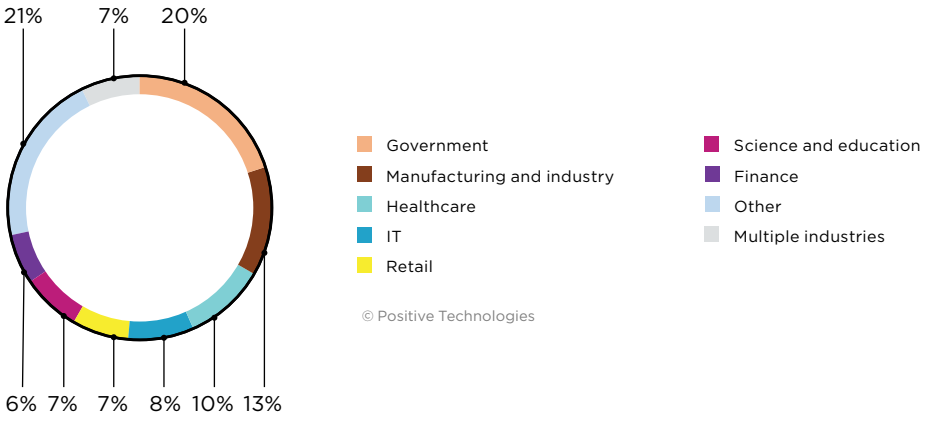


*Figure 4. Victim categories among organizations in Q4 2020*

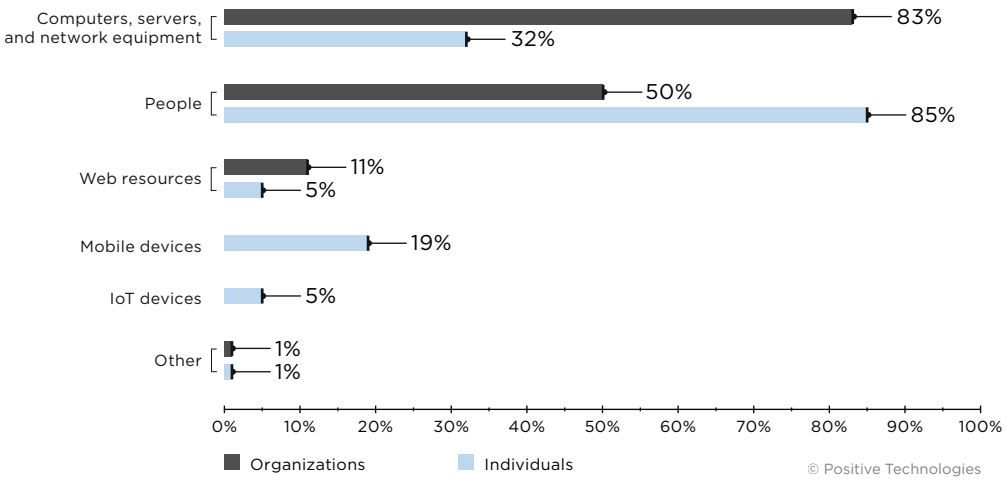


*Figure 5. Attack targets (percentage of attacks)*

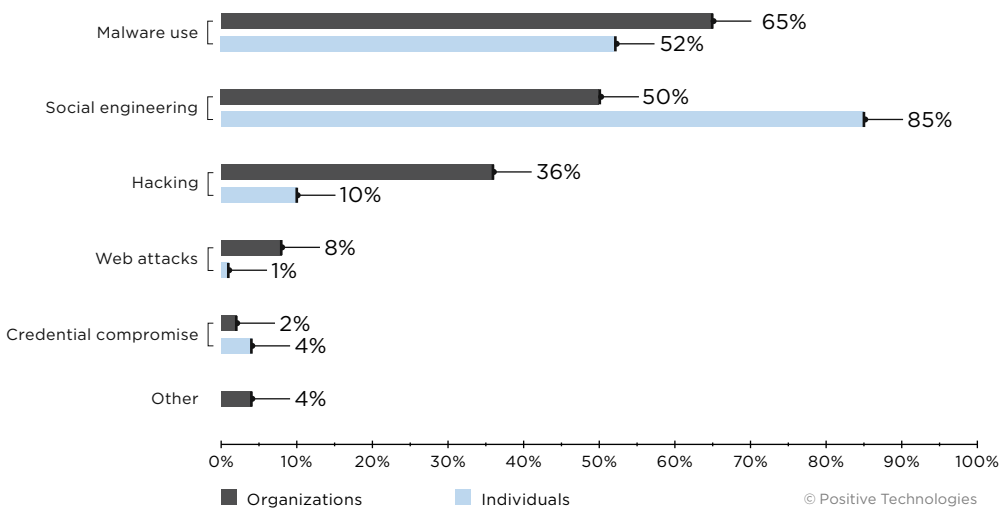


*Figure 6. Attack methods (percentage of attacks)*

© Positive Technologies

**Victim categories**

| Per-industry classification of cyberincidents by motive, method, and victim categories | | Government | Finance | Manufacturing and industry | Healthcare | IT | Science and education | Retail | Other | Multiple industries | Individuals |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Total** | **108** | **29** | **68** | **55** | **40** | **37** | **39** | **112** | **39** | **73** |
| **Target** | Computers, servers, and network equipment | 94 | 26 | 66 | 48 | 33 | 28 | 28 | 84 | 28 | 23 |
| | Web resources | 11 | 1 | 1 | 2 | 3 | 1 | 12 | 21 | 4 | 4 |
| | People | 49 | 15 | 43 | 40 | 18 | 24 | 13 | 40 | 24 | 62 |
| | Mobile devices | 1 | | | | | | | 1 | | 14 |
| | IoT devices | | | | | | | | | 1 | 4 |
| | Other | | | | | | 2 | 1 | 4 | | 1 |
| **Method** | Malware use | 68 | 18 | 58 | 43 | 26 | 20 | 22 | 62 | 26 | 38 |
| | Social engineering | 49 | 15 | 43 | 40 | 18 | 24 | 13 | 40 | 24 | 62 |
| | Credential compromise | | | | | 1 | 2 | 1 | 5 | 3 | 3 |
| | Hacking | 41 | 12 | 24 | 14 | 16 | 7 | 16 | 50 | 11 | 7 |
| | Web attacks | 10 | 1 | 1 | 1 | | 1 | 9 | 16 | 3 | 1 |
| | Other | 9 | 1 | | | 6 | 3 | | 2 | | 1 |
| **Motive** | Access to information | 52 | 22 | 55 | 32 | 24 | 19 | 33 | 57 | 27 | 51 |
| | Financial profit | 39 | 10 | 19 | 39 | 16 | 19 | 13 | 56 | 9 | 22 |
| | Hacktivism | 24 | 2 | 7 | 3 | 10 | 9 | 2 | 16 | 9 | 5 |
| | Cyberwar | 3 | 1 | | | | | | 1 | | |
| | Unknown | 1 | | | | | | | 2 | | |

Darker colors indicate a greater proportion of attacks within a particular victim category

0% 10% 20% 30% 40% 100%

# Malware attacks

Throughout the year, we noted continuous growth in malware attacks. In Q4 2020, we saw a slowdown in the explosive growth in ransomware attacks from Q3. The share of ransomware attacks increased by 5 percentage points versus the previous quarter, to 56 percent. During the year we also saw the active use of spyware in attacks against individuals.

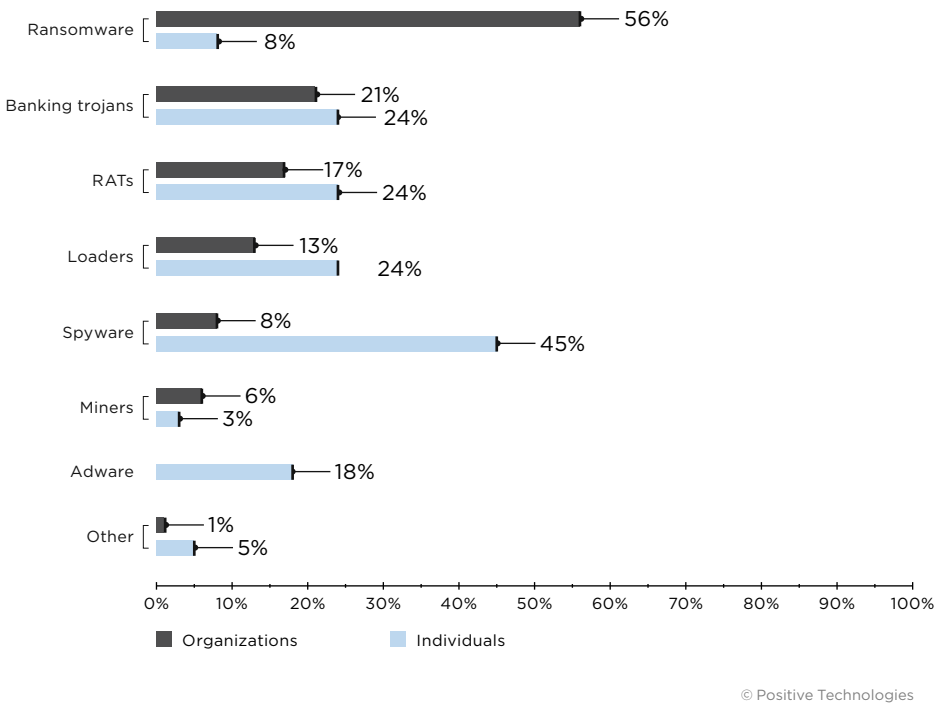


*Figure 7. Malware types (percentage of attacks involving malware)*

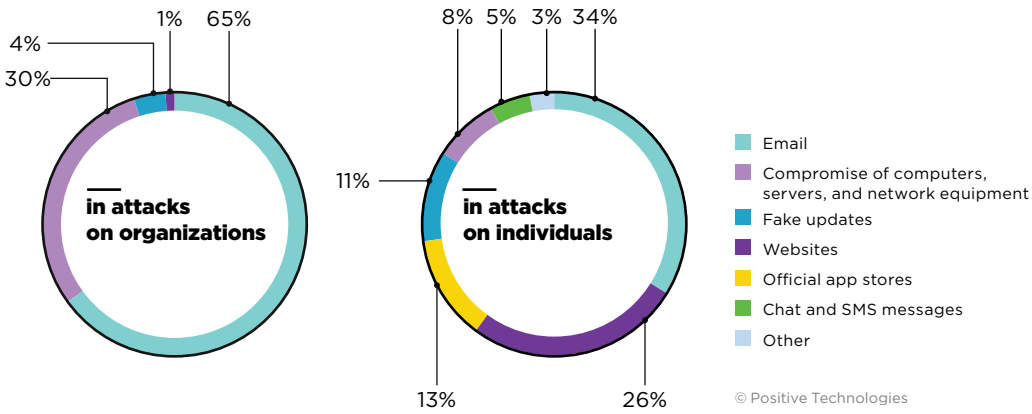


*Figure 8. Methods used for malware distribution*

In attacks on organizations, the most frequent method used to spread malware (in 30% of cases) was exploitation of vulnerabilities in IT infrastructure and protection flaws. For example, during Q4 hackers actively exploited an Oracle WebLogic server vulnerability (CVE-2020-14882) that allowed remote code execution, though a patch was released in early October. One hacker attack was aimed at deploying Cobalt Strike Beacons, which allow persistent remote access to compromised hosts. This access later allowed attackers to collect data and deploy second-stage malware. Another wave of attacks involved the distribution of DarkIRC malware. DarkIRC comes with a multitude of capabilities, including remote access, keylogging, DDoS attacks, and bitcoin clipping, and can be spread on networks by brute-forcing credentials to Microsoft SQL Server and RDP, as well as over SMB or via USB devices. An interesting thing about DarkIRC is that before unpacking, it first checks if the host is running in a VMware, VirtualBox, VBox, QEMU, or Xen virtual machine and then stops the infection process if it detects a sandbox environment.

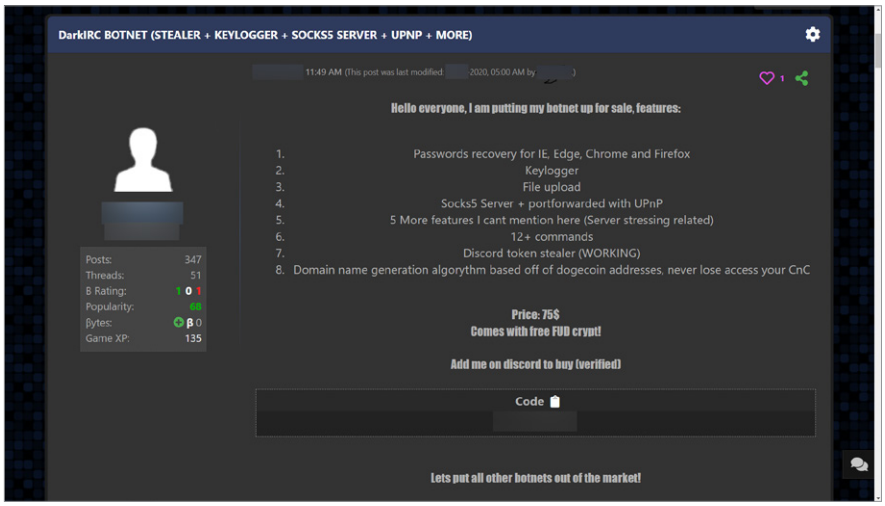


*Figure 9. DarkIRC for sale on the darkweb*

Social engineering remains an ever-present hazard. In 65 percent of attacks on organizations, the first stage relied on the human factor. Many such attacks involved the Emotet trojan. After a lull, the trojan re-emerged in full force in mid-2020. In Lithuania, for example, hackers used the trojan in attacks against several municipalities and the National Center for Public Health (NVSC). In other attacks targeting a broader audience, hackers sent phishing emails that pretended to be messages from Windows Update, shipping information, resumes, COVID-19 information, and even invitations to a Halloween party. As usual, the emails contained malicious Microsoft Word (.doc) attachments that, once opened, try to trick the user into enabling macros. The main distinguishing feature of this campaign is that once macros are enabled, the user gets a fake error message about Word having experienced an error trying to open the file. This put users off their guard, and the malware can start executing its payload.

Just as interesting and as dangerous, the BazarLoader trojan made a splash in Q4. The trojan is used to obtain remote access to a victim's computer and deploy Ryuk ransomware. In early October, researchers at cybersecurity firm ProofPoint spotted a new phishing campaign that capitalized on interest in the health of Donald Trump. The malicious emails asked victims to download a Google document by clicking an embedded link. Clicking the link downloaded the BazarLoader executable to the victim's computer. Mid-October saw a new wave of phishing emails that distributed BazarLoader using public links to the Basecamp web-based project management platform. Basecamp allows users to upload all types of files to a project, including executables, which is convenient for attackers. Cybersecurity firm Cyjax reported that in addition to malware distribution, hackers can also use Basecamp in phishing attacks to steal login credentials.

# New ransomware boom

Medical and government institutions, as well as industrial companies, bore the brunt of ransomware attacks.

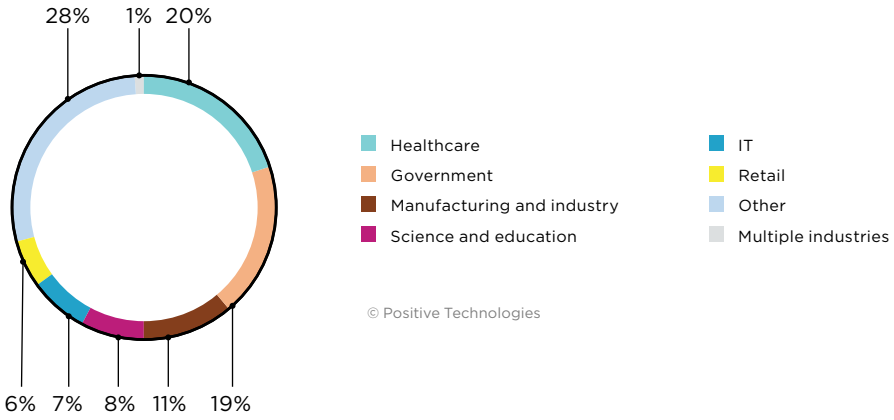


*Figure 10. Ransomware attacks by industry*

Besides conducting attacks, hackers also created their own sites for publishing stolen data, such as the News & Leaks data leak site by the Mount Locker group. Some also formed alliances with other gangs. For example, Ako and ThunderX ransomware operators joined under the name Ranzy Locker.

***Top 5 ransomware families***

1. Ryuk (Conti)
2. REvil
3. Clop
4. Egregor
5. DoppelPaymer

Operators of Ryuk ransomware attacked medical institutions most frequently in Q4 2020. The victims included Wyckoff Heights Medical Center in Brooklyn, the University of Vermont Health Network, Sky Lakes Medical Center in Klamath Falls (Oregon), St. Lawrence Health System (New York), a gastroenterology clinic in Nevada, and Taylor Made Diagnostics. Attacks on medical institutions can have devastating consequences. For example, electronic health records for cancer patients went down after a cyberattack on the University of Vermont Health Network. The system was restored only a month after the attack, forcing clinicians to attempt to recreate chemotherapy protocols from memory in the meantime.

However, Ryuk operators target other industries as well. FS-ISAC describes Ryuk as a "rapidly evolving threat" to financial institutions. An incident with payment card processing giant Total System Services is a notable example. The third-largest payment processor for financial institutions in North America was hit by a ransomware attack in early December. More than 10 GB of data was published as a result of the attack.

In one Ryuk ransomware incident investigated by DFIR experts, the attackers managed to compromise an entire corporate network with the ransomware in just two hours. The attackers exploited vulnerability CVE-2020-1472 for the initial attack vector. On average, it takes ransomware operators from two to five days to perform an attack.

A new ransomware operator known as Hades debuted in early December. The first reported incident took place on December 15, when trucking and freight logistics company Forward Air suffered a ransomware attack. The attack caused disruption and service delays, since cargo documentation was stored electronically. Nine days after the Forward Air incident, news came of an attack on logistics provider OmniTRAX. This attack was attributed to the Conti ransomware gang. The hackers stole over 70 GB of internal documents. OmniTRAX refused to pay the ransom.

Security experts warn against paying off ransomware attackers, since doing so encourages future crimes and justifies the continued investment of time and effort. However, not all companies follow these recommendations; some of them agree to pay up. In Q4 2020 alone, several companies paid a ransom, including online educator K12, hit by Ryuk ransomware in mid-November; Barbados-based conglomerate Ansa, attacked by REvil in October; a Mississippi school district; and Delaware County (Pennsylvania), hit by DoppelPaymer ransomware. The last two victims paid attackers $300,000 and $500,000, respectively.

First observed in September 2020, Egregor ransomware made a name for itself at the end of the year. Prominent victims included transportation agency TransLink, Chile-based multinational retailer Cencosud, U.S. department store Kmart, game developers Ubisoft and Crytek, U.S. bookstore giant Barnes & Noble, and major staffing agency Randstad. At Barnes & Noble, the stolen data included financial and audit documents as well as client information, including shipping addresses, email addresses, and purchase history. As a result of the attack on Cencosud, the company's customers were temporarily unable to use Cencosud Card credit cards, make returns, or pick up web purchases.

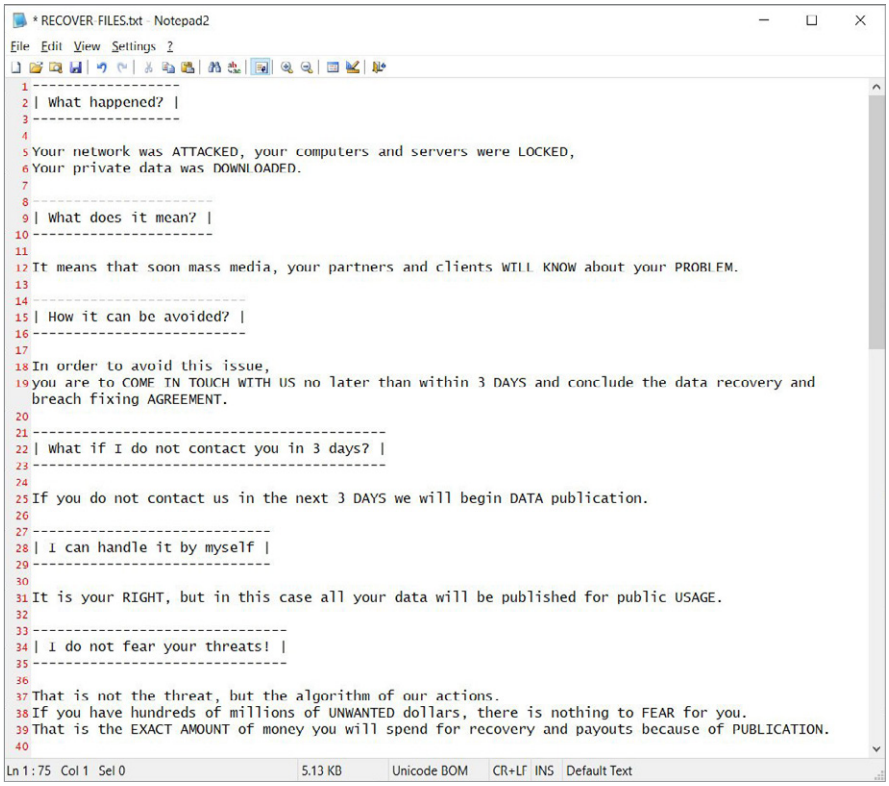


*Figure 11. Egregor ransom note*

Nor did ransomware operators spare resorts. In late October, U.S. ski and golf resort operator Boyne Resorts suffered a WastedLocker ransomware attack. The company's reservations system was down for days as a result.

In November, web hosting provider Managed.com was attacked by REvil ransomware. The company's web hosting systems were unavailable for at least four days. The attack impacted client sites. Managed.com said the attack took down its entire infrastructure, including WordPress and DotNetNuke managed hosting solutions, mail servers, DNS servers, RDP access points, FTP servers, and online databases. The hackers demanded a $500,000 ransom.

# Attacks on the industrial sector

Industrial companies have remained the second-most popular target for the last two years. In Q4 2020, a third of attacks on the industry involved hacking, and 84 percent of attacks were performed using malware.

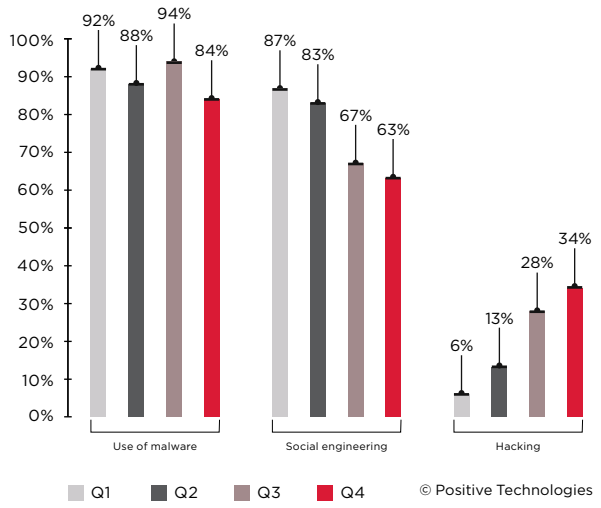


*Figure 12. Main attack methods in 2020 (percentage of attacks on industrial companies)*

The PT Expert Security Center recorded an uptick in attacks by the RTM group: 61 phishing mailings from them targeted the industrial sector, among others. Banking trojans, which previously had been used in 33 percent of attacks against industrial companies, grew to account for 59 percent of total malware attacks.

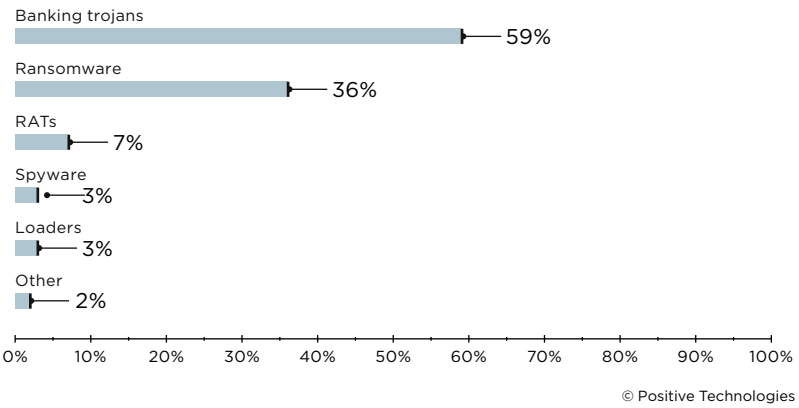


*Figure 13. Types of malware in attacks on industrial companies (percentage of malware-related attacks)*

Two airplane makers hit ransomware turbulence in Q4. RansomExx attacked Brazilian company Embraer. The attackers stole and later published employee details, contracts, flight simulation data, and other confidential information. Next, operators of Ragnar Locker ransomware breached Dassault Falcon Jet's network and encrypted the company's systems by exploiting vulnerability CVE-2019-19781 in Citrix Application Delivery Controller. The hackers stole trade secrets, including documents pertaining to the development of a new Falcon 6X business jet.

By persisting on the company's network for over half a year, they were able to thoroughly study the infrastructure and strike the most sensitive targets.

Dassault Falcon Jet is not the only major victim of Ragnar Locker. On November 1, Italian liquor company Campari Group joined the list of victims. Attackers made off with 2 TB of data, including bank statements, emails, and trade secrets. They demanded a ransom of $15 million. In return, they promised to provide a decryptor, not to publish the stolen data, and even provide a network penetration report and recommendations on how to improve security.

The DoppelPaymer ransomware gang demanded an even greater ransom—a whopping $34 million—to decrypt systems and keep quiet after an attack on electronics manufacturer Foxconn. The attackers stole more than 100 GB of data. Interestingly, they made a point of stating that they had targeted only Foxconn servers, avoiding employees' workstations.

Attackers did not leave out energy companies, either. A cyberattack on October 13 in Mumbai caused a two-hour power outage. Attackers targeted the city's load dispatch center. The outage disrupted operations at the stock exchange and other establishments across Mumbai, Thane, and Navi Mumbai, and led to the cancellation of train services. Mumbai hospitals shut down all non-ICU patient care. In mid-November, energy company Parkland in Calgary (Canada) was attacked by the operators of Clop ransomware. The stolen information included sensitive documents related to refinery operations as well as personal data, such as a scan of one of the directors' passports. At The Standoff cyber-range in November 2020, theft of sensitive documents from an oil refinery constituted one of the most frequently triggered risks.

In November 2020, attackers hacked a water reservoir SCADA system in Israel. With such access, attackers can freely modify the operating parameters of critical infrastructure. They could, for example, increase the water pressure in the reservoir (causing it to burst) or increase the temperature to critical levels. Lack of authentication and direct connection of ICS devices to the Internet made the hack possible. After attackers published a video of the breach, authentication was turned on but the system remained Internet-accessible, meaning that hackers could strike again.

# Supply chain attacks

Software vendors were another "trendy target" in Q4. The most prominent incident targeted SolarWinds clients, including the U.S. Department of State, Microsoft, Cisco, and FireEye. In a supply chain attack, attackers penetrated the SolarWinds network and added a malicious backdoor into updates for the company's Orion platform. Around 18,000 clients installed the tainted update on their systems. Of note, the attackers managed to steal penetration testing tools from cybersecurity firm FireEye. The stolen software contains exploits for numerous vulnerabilities, which attackers will likely leverage in future campaigns.

In November, domain name registrar GoDaddy fell victim to a phishing attack. The attackers duped employees into changing registration records of several clients, including cryptocurrency exchanges NiceHash and Liquid. The changes allowed redirecting user traffic to attacker-controlled servers.

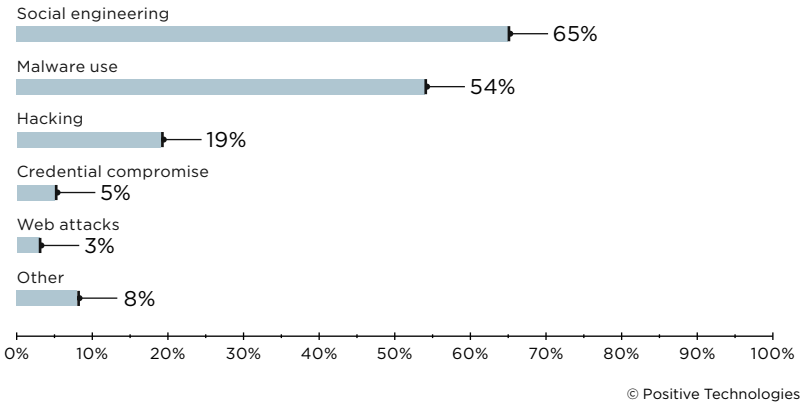


*Figure 14. Attack methods (percentage of attacks on IT companies)*

Social engineering was especially popular in Q4, accounting for 65 percent of all attacks against IT companies. In one such case, the website of Japanese game developer Koei Tecmo was hacked and data for 65,000 users was stolen through a phishing email sent to an employee. The threat actor attempted to sell access (in the form of a backdoor) and a forum user database for $7,800. Five days later, however, the database was posted online free of charge.

Another Japanese game giant, Capcom, was hit by Ragnar Locker ransomware in early November. Capcom flatly denied that customer data had been accessed, but the ransomware operators published confirmation on their website. The criminals stole personal information of Capcom employees (including former employees), such as passport information, as well as data for customers and business partners, sales reports, development documents, and other confidential information. Ransomware attacks on IT companies did not stop there. In late December, hacking group Pay2Key attacked Israeli cybersecurity firm Portnox. Before encrypting the IT infrastructure, the group stole confidential information, including documents related to Portnox's clients. They even published a security audit of Elbit, a major Israeli defense company. A total of 1 TB of data was stolen.

Software AG, Germany's second-largest software vendor, fell victim to a Clop ransomware attack. Company files and employee information were compromised. The criminals demanded a $23 million ransom for non-disclosure of the stolen data.

# Dangerous shopping

The number of attacks on retail and commerce increased by 56 percent compared to Q3, reaching a new high for the last two years.

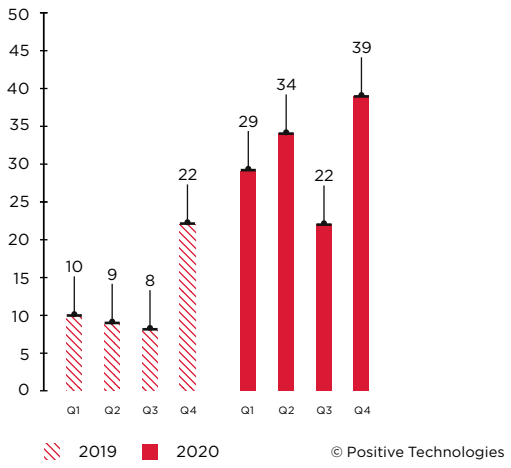


*Figure 15. Number of attacks on retail and commerce*

When attacking retail and commerce, threat actors are typically seeking payment card data, which accounted for 33 percent of all data stolen in Q4. Other targets include customers' personal data (27%) and credentials (20%).

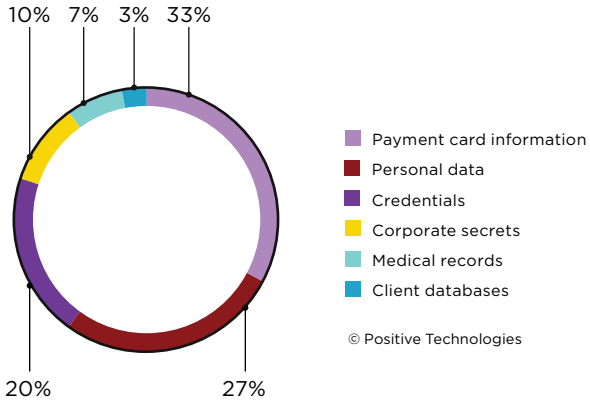


*Figure 16. Data stolen in attacks on retail and commerce*

Ransomware was used in 31 percent of incidents. One notable example is the attack on South Korean retailer E-Land on November 22. The ransomware operator had persistence on the company's network for more than a year. During this time, they exfiltrated credit card data with the help of POS malware. The company learned of the data breach only after the ransomware attack. As a result, E-Land was forced to shut down 23 stores. Attackers failed to capture CVCs and CVVs, but the amount of stolen data is enough to create fake cards.

Magecart attacks accounted for 23 percent of incidents. The most interesting thing about these attacks is how they are made stealthy. For example, researchers at cybersecurity company Sansec discovered web skimmers inside CSS code on the sites of three different online stores. This tactic is useful for evading detection, since CSS code is not commonly checked by security scanners and will most likely escape attention during manual audits. The skimmer script launched only when customers of compromised sites started to enter payment or personal information.

Sansec discovered another sophisticated stealth method, involving hiding a malicious payload in social media SVG sharing icons. The code of the skimmer script is loaded as an HTML element. A separate decoder can be deliberately deployed somewhere else because if only one of the malware components is found, an infosec expert may conclude that the malware is inactive.

Malefactors did not pass up Black Friday: a self-healing skimmer was discovered on over 50 online stores. On the compromised sites, the skimmer script showed a fake payment form and then sent all of the intercepted data to the real checkout page. The transaction process was virtually indistinguishable from the real thing, so security systems did not raise any flags. For robust persistence, attackers placed four payload components on the hacked websites:

1) Backdoor loader, to install the skimmer
2) Backdoor watchdog, to restore the backdoor in the event of detection and deletion
3) Web skimmer
4) Infostealer, to steal administrator credentials

Therefore, even if the entire infection and healing chain were to be discovered, the infostealer would still provide continuous access to servers, allowing the attackers to deploy all the payload components a second time. The infection became possible in the first place only because all the compromised stores were running Magento versions 2.2.3–2.2.7, despite being urged to upgrade to a more recent version.

Even when criminals do not manage to hack online stores, customers may still not receive products due to attacks on other links in the supply chain, such as delivery. One such incident struck Russian delivery service PickPoint on December 4. Attackers hacked the company's network of package lockers, remotely opening 2,732 lockers in Moscow and St. Petersburg. The process of restoring systems took several days.

# Pre-election happenings

In late 2019, Positive Technologies experts shared their forecasts about cybersecurity trends for 2020. They expected many cyberattacks in the run-up to the U.S. presidential elections, including against the sites of political parties and candidates. This is, indeed, what happened.

In late October, hackers stole $2.3 million from the account of the Wisconsin Republican Party. Criminals manipulated invoices from four of the party's direct mail and merchandise vendors. Also in Wisconsin, a spokeswoman for the state's Democratic Party said there had been more than 800 attempts to phish for financial gain during the most recent election cycle, but none were successful.

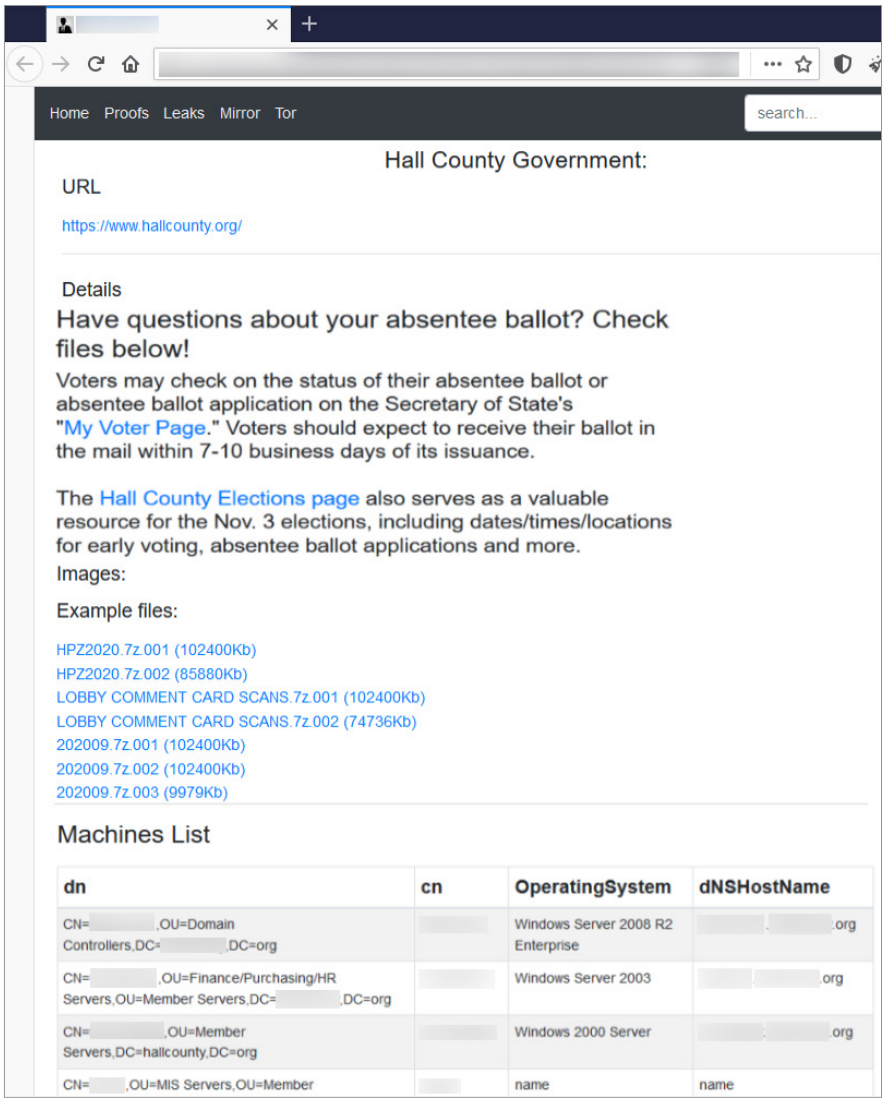


*Figure 17. Announcement regarding Hall County data stolen by DoppelPaymer ransomware*

Cyberattacks hit not only those in power, but also ordinary people. On October 7, the DoppelPaymer ransomware gang stole data on voters in the state of Georgia in an attack on the network and phone systems of Hall County. In early November, a phishing attack was spotted in which Qbot malware was distributed in a file allegedly containing information about election interference. Once on a victim's computer, Qbot starts grabbing user data and email messages for use in later attacks.

Election support systems fell prey to attacks exploiting vulnerability CVE-2018-1337 in the FortiOS SSL VPN and Windows vulnerability CVE-2020-1472.

The criminals behind Emotet malware got in on the act as well. In an October phishing campaign, they sent emails purporting to come from the U.S. Democratic National Committee. The emails claimed to be looking for volunteers, with an attachment promising further information. But in reality, opening the attachment triggered a message that the file was created on an iOS device and prompted users to "enable content" in order to view the file. Once a user enabled content, the infection process started.

# One thousand and one ways to exploit COVID-19

The share of social engineering attacks that made use of the pandemic remained the same as in Q3: 4.6 percent. Despite the abundance of materials available online about COVID-19, attackers still manage to lure victims into opening phishing emails with the promise of valuable information. In one such attack, a phishing email disguised as an automatic message from SharePoint linked to a document supposedly informing of pandemic-related requirements. Clicking the link led victims to an attacker-controlled site.

Another popular ruse was financial relief. In late October, fraudsters sent messages purporting to come from the International Monetary Fund claiming that 125 beneficiaries had been shortlisted for compensation. All users had to do to receive this bounty was to reply with their private email address and provide additional information if requested. The goal was to collect as much user information as possible. The attack was masked to evade detection: the message did not contain any links, the "reply-to" address differed from the sender address, and the message was made to look like part of an email thread.

In December, fraudsters impersonated the New York Department of Labor to offer $600 in pandemic relief. To receive the money, users were asked to enter their personal data in a special form.

In yet another phishing attack, messages claimed to contain COVID-19 test results. The email contained a password-protected RAR file with malware inside. This is another time-proven stealth technique, since not all security tools can scan encrypted RAR files.

Interest in COVID-19 vaccines was targeted in 40 percent of all phishing attacks in Q4. A vivid example is the December phishing campaign discovered by KnowBe4 security researchers. The campaign was propelled by reports that a vaccine manufacturer might not be able to supply additional vaccine doses to the U.S. Tapping into panic and confusion, hackers sent messages asking users to fill out a form in order to get on a vaccine list. When users clicked the included link, they were redirected to a phishing site that pretended to be a legitimate cloud service asking users to sign in.

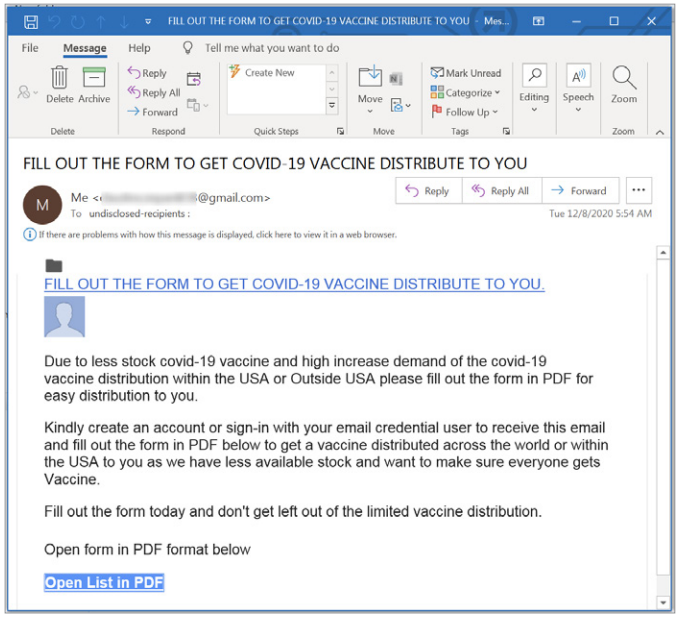


*Figure 18. Sample of a vaccine-themed phishing email*

COVID-19 vaccines interest both ordinary Internet users and cybercriminals. Throughout the quarter, we observed attacks on vaccine production and supply chains. Pharmaceutical companies, such as Fareva, Dr. Reddy's, Johnson & Johnson, Novavax, Genexine, Shin Poong Pharmaceutical, Celltrion, and AstraZeneca, came under a barrage of attacks. U.S.-based cold storage giant Americold, whose facilities have considerable importance for vaccine storage, was not spared either: sources said the company was hit by a ransomware attack. Cyberattacks also target government agencies involved in making vaccine-related decisions. In early December, the European Medicines Agency was hit by a cyberattack in which documents of vaccine developers Pfizer and BioNTech were stolen.

# About the research

In this quarter's report, Positive Technologies shares information on the most important global IT security threats. Information is drawn from our own expertise, outcomes of numerous investigations, and data from authoritative sources.

In our view, the majority of cyberattacks are not made public due to reputational risks. The result is that even organizations that investigate incidents and analyze activity by hacker groups are unable to perform a precise count. This research is conducted in order to draw the attention of companies and ordinary individuals who care about the state of information security to the key motives and methods of cyberattacks, as well as to highlight the main trends in the changing cyberthreat landscape.

In this report, each mass attack (in which attackers send out a phishing email to many addresses, for instance) is counted as a single incident. Definitions for terms used in this report are available in the glossary on the Positive Technologies site.