# Cybersecurity threatscape Q4 2021


Positive Technologies

ptsecurity.com

# Contents

# Summary

Highlights of Q4 2021 include:

- In Q4, the number of attacks increased by 7.2 percent against the previous quarter, which was caused by a rise in the number of ransomware attacks after a decline in Q3.
- The volume of targeted attacks on organizations dropped by 6 percentage points against the previous quarter (75% and 69% in Q3 and Q4, respectively).
- The share of attacks targeting individuals climbed slightly to 16 percent versus 14 percent in the previous quarter. Cybercriminals continue to hunt for individual users' confidential information: 73 percent of attacks led to leakage of such information, which is up 11 p.p. on Q3.
- Ransomware operators, facing pressure from law enforcement and the blocking of topics on special forums, have had to band together and pool their experience in order to regain their footing in the cybercrime arena. All this led to a significant fall in the share of attacks on government institutions (10% versus 21% in Q3), which in Q4 were subjected to more APT attacks and leaks of confidential information.
- Attacks on organizations involving the use of remote access trojans (RATs) continues to grow—from 36 percent in Q3 to 39 percent in Q4. At the same time, the number of botnet-related attacks increased significantly, with a record-breaking magnitude of DDoS attacks being logged.
- Cybercriminals are trying out new methods to hoodwink email filtering tools (the most common malware delivery channel) and using the popular social platform Discord to distribute malware and set up C2 servers.
- The uptick in supply chain attacks, ongoing since late 2020, was again prominent in Q4.
- The most frequently attacked sector in Q4 was healthcare. More than half of all attacks disrupted the operation of medical institutions. The cause was ransomware, which was used in 83 percent of malware attacks.
- In the industrial sector, we noted the return of ransomware after a lull: the share of ransomware attacks increased from 32 percent in Q3 to 56 percent in Q4.
- Attacks disrupted the core business of industrial organizations in 50 percent of cases, up 31 p.p. on Q3. In 42 percent of attacks, organizations faced leakage of confidential information.

To guard against cyberattacks, we recommend following our guidelines on personal and corporate security. We strongly advise installing security updates in a timely manner, monitoring network traffic, investigating information security incidents to identify points of compromise and infrastructure vulnerabilities, promptly responding to such incidents, and eliminating the causes and consequences. You can strengthen security at the corporate perimeter with the aid of cutting-edge security tools, such as web application firewalls for protecting web resources. To prevent malware infection, we recommend using sandboxes to analyze the behavior of files in a virtual environment and detect malicious activity.

# Statistics

Q4 2021 saw a 7.2 percent rise in the number of cyberattacks against the previous quarter. We attribute this growth to the recovery of ransomware (as signaled by the 7 p.p. rise in the share of attacks on computers, servers, and network equipment) and attackers' active exploitation of network infrastructure vulnerabilities (38% versus 33% in Q3 2021). Most often, the targets were medical organizations, government agencies and industry.

In addition, we see a rise in the number of mass phishing campaigns, and attacks on individual mobile devices: social engineering was used in 90 percent of cases, while mobile devices were targeted 9 p.p. more than in the previous quarter. In Q4, organizations encountered 6 p.p. more leaks of confidential information than in the previous quarter, and individuals 11 p.p. Cybercriminals primarily targeted personal data and account credentials. This data can be used to gain access to victims' accounts and in attacks on corporate systems.

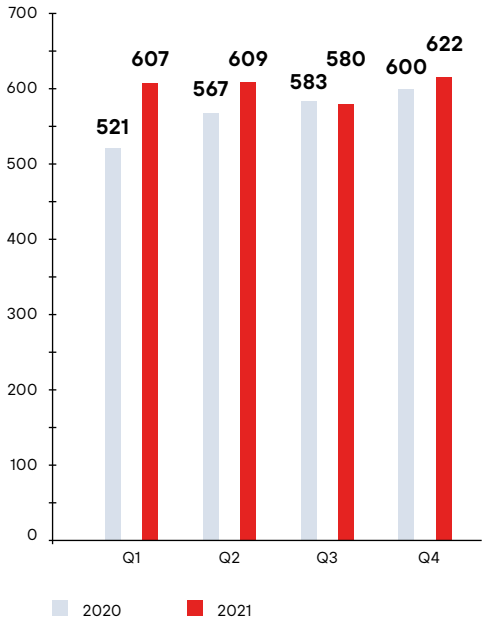


*Figure 1. Number of attacks in 2020 and 2021 (by quarter)*

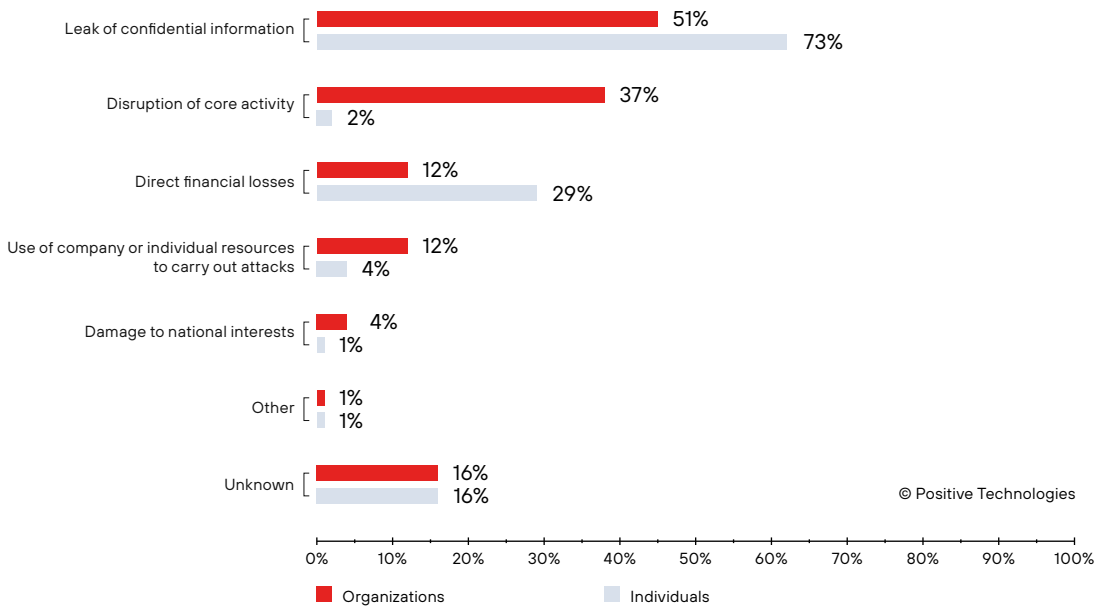


*Figure 2. Attack consequences (share of attacks)*

## 69% of attacks were targeted

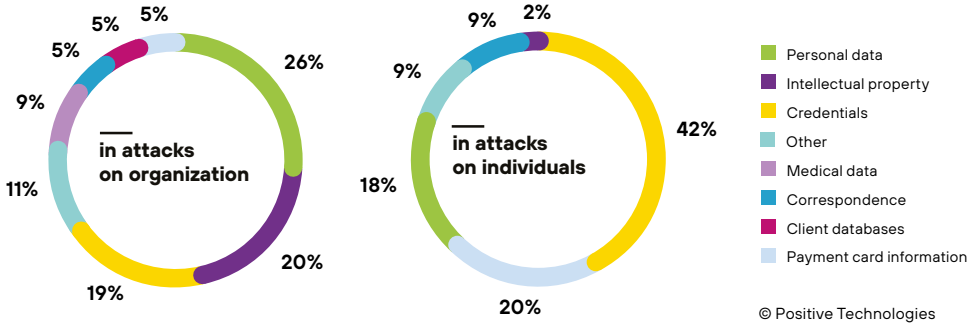


*Figure 3. Types of data stolen*

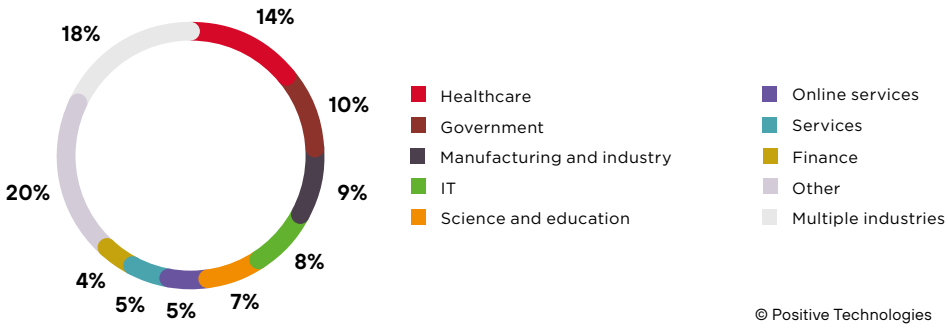


*Figure 4. Victim categories among organizations*

## 16 percent of attacks were aimed at individuals

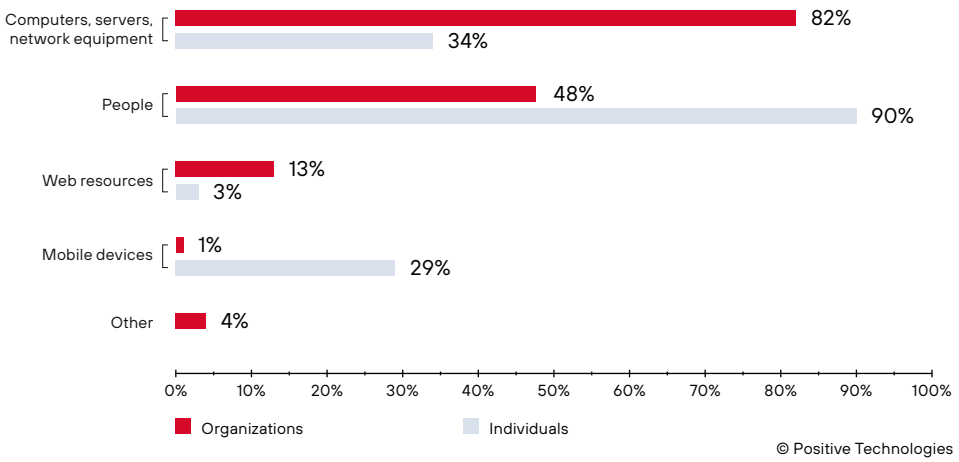


*Figure 5. Attack targets (percentage of attacks)*

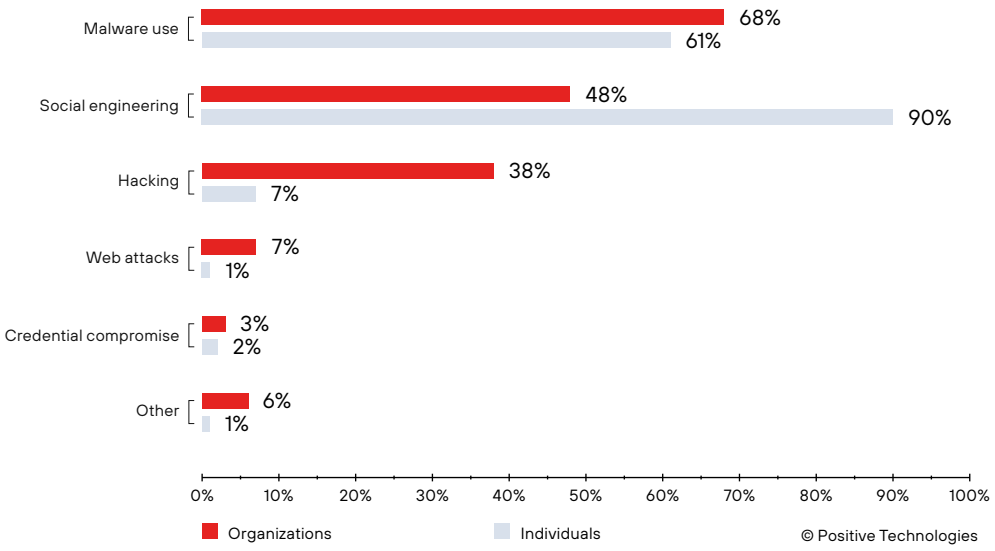


*Figure 6. Attack methods (percentage of attacks)*

Sector

© Positive Technologies

| | Per-industry classification of cyberincidents by motive, method, and target | Government | Finance | Manufacturing and industry | Healthcare | IT | Science and education | Online services | Services | Other | Multiple industries | Individuals |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Total** | **51** | **19** | **48** | **73** | **43** | **37** | **28** | **24** | **106** | **94** | **99** |
| **Target** | Computers, servers, network equipment | 42 | 13 | 46 | 60 | 42 | 31 | 17 | 22 | 82 | 75 | 34 |
| | Web resources | 7 | 3 | | 5 | 1 | 6 | 21 | 1 | 15 | 7 | 3 |
| | People | 26 | 15 | 26 | 48 | 16 | 22 | 1 | 11 | 42 | 46 | 89 |
| | Mobile devices | | | 1 | | | | | | | 4 | 29 |
| | Other | | | | | | | | | 12 | 7 | |
| **Method** | Malware use | 33 | 12 | 43 | 48 | 34 | 24 | 3 | 15 | 70 | 72 | 60 |
| | Social engineering | 26 | 15 | 26 | 48 | 16 | 22 | 1 | 11 | 42 | 46 | 89 |
| | Credential compromise | 3 | | 1 | 4 | 1 | 3 | 1 | | 5 | | 2 |
| | Hacking | 17 | 3 | 21 | 19 | 27 | 9 | 7 | 12 | 46 | 38 | 7 |
| | Web attacks | 4 | 2 | | 2 | | 4 | 11 | 1 | 7 | 5 | 1 |
| | Other | | | | | | | 9 | | 13 | 9 | 1 |
| **Consequences** | Leak of confidential information | 22 | 12 | 20 | 45 | 24 | 20 | 16 | 14 | 58 | 35 | 72 |
| | Disruption of core activity | 15 | 6 | 24 | 38 | 16 | 20 | 16 | 13 | 32 | 11 | 2 |
| | Direct financial losses | 4 | 5 | 9 | 5 | 2 | 3 | 2 | 4 | 24 | 6 | 29 |
| | Damage to national interests | 10 | 1 | 4 | 1 | | 1 | | | 2 | | 1 |
| | Use of company or individual resources to carry out attacks | 2 | 3 | 7 | | 9 | | | 2 | 5 | 33 | 4 |
| | Other | 1 | 1 | | | | 1 | 1 | | | | 1 |
| | Unknown | 10 | 2 | 3 | 4 | 4 | 4 | 1 | 4 | 21 | 29 | 16 |

Color gradation shows shares of attack within one metric for each category of victims.

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

# Malware: new techniques

The share of malware use remains practically unchanged since the previous quarter, 53 percent. The leader in malware attacks on organizations is still ransomware. RATs have become more common, possibly due to the expansion of botnets.

Cybercriminals make active use of spyware in attacks on individuals. This trend was observed throughout the year: the share of these malicious programs rose by 17 p.p. from Q1.

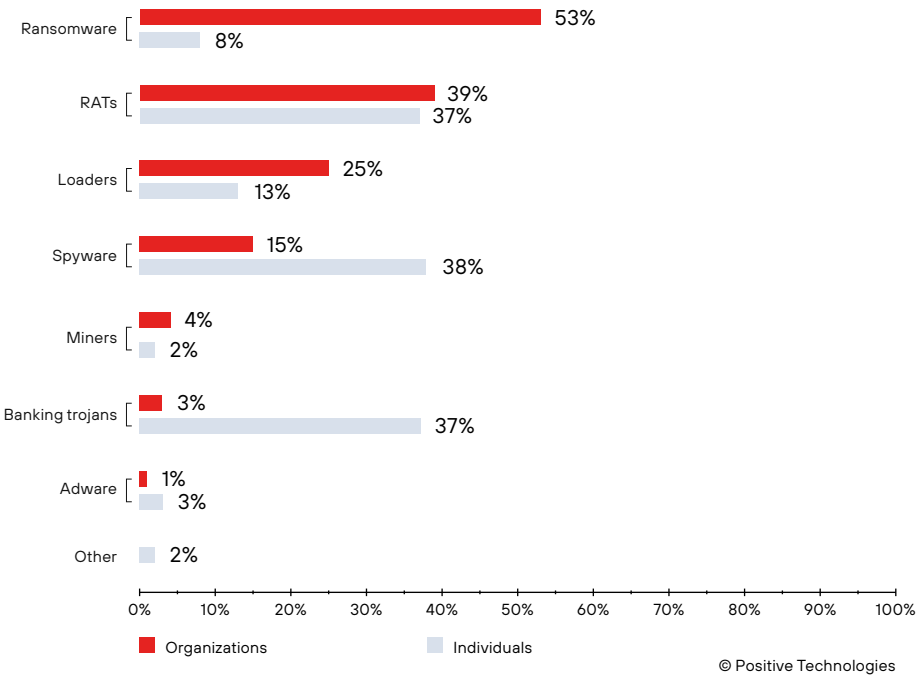


*Figure 7. Types of malware (share of malware attacks)*

**Like peas in a pod**

The most common malware distribution channel among organizations is email, which was used to deliver more than half of all malware. Many APT groups continue to use this channel in their attacks. In Q4, PT Expert Security Center (PT ESC) identified malicious mailings from APT37, Cloud Atlas, and TA428. Attackers are also trying out new ways to trick anti-spam systems. A notable case was the detection by INKY analysts of a phishing notification about a Verizon voicemail message: in the email, the logo of the telecommunications giant was replaced with a mathematical square root symbol, which allowed the attackers to bypass anti-spam filtering tools and redirect victims to a phishing site that asked for their credentials.

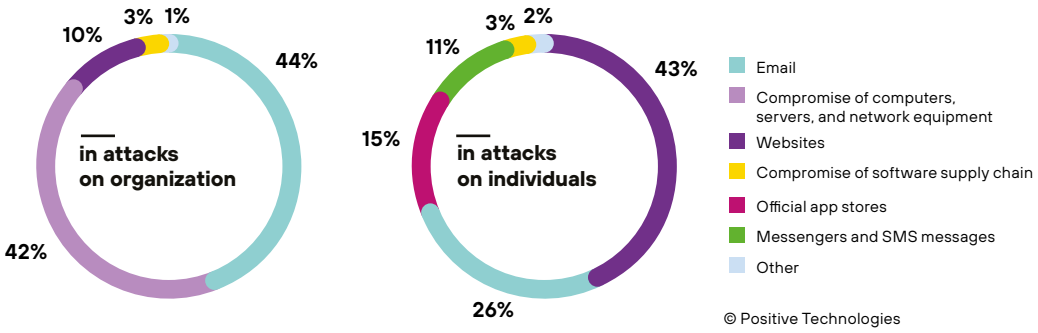


*Figure 8. Malware distribution methods (share of malware attacks on organizations)*

### Scope of attacks

In Q4, cybercriminals took to Discord, a VoIP, instant messaging, and digital distribution platform with a worldwide audience of 140 million, to distribute malware. Experts at RiskIQ and Check Point discovered that attackers were abusing the content delivery network to spread various forms of malware.

RiskIQ investigated Discord links ending in specific file extensions (e.g. executables, DLLs, compressed files, documents) and concluded that over 100 Discord URLs were used to deliver 27 unique families of four malware types: backdoors, credential stealers, spyware and RATs. One group of attackers that used the content delivery network to distribute malware on the Discord servers of the NFT and DeFi communities is BabaDeda.

Check Point found that, by integrating malicious code into the Discord Bot API, a bot management tool, the attackers had turned the latter into an RAT to gain full access over the device, and the Discord server into a C2 server. Through the Python API wrapper for Discord, the bot provides a token for processing incoming messages on a predefined Discord server, and then executes on the victim's device the attacker's commands received by this server.

Discord is a cross-platform app, its traffic is encrypted and classified as legitimate, and Discord-based malware does not require the app itself to be installed or running, all of which makes Discord-based RATs flexible and hard to detect.

### Smiling spyware

The developers of the Joker spyware for Android have managed to infect almost half a million devices worldwide, reports Pradeo. Disguised as seemingly harmless apps on Google Play, Joker can browse through contacts, steal messages with confirmation codes and device information, take out costly subscriptions, and send stolen information to a remote server.

# The calm before the storm?

U.S. Treasury sanctions and the recent arrest and exposure of the REvil group have not deterred cybercriminals, and after a brief lull in Q3 operators and developers resumed their global attacks on organizations. The attack figures are similar to those in Q1 2021, which was followed by an explosion in the number of ransomware attacks.

Many companies have stopped paying ransoms to attackers. In the U.S., after a string of major ransomware attacks that had severe economic and security repercussions, the Department of Justice began treating ransomware attacks with the same priority as terrorist attacks ([1], [2]). A third of respondents in a Venafi survey of IT security decision-makers said they would pay up, but 57 percent would refuse if they had to publicly disclose the ransom payment—the U.S. Senate recently introduced the Ransomware Disclosure Act, requiring companies to report payments to ransomwarers within 48 hours. Another factor causing companies to think twice about paying up is consumers' negative attitude: a report by Cohesity shows that 47 percent of those surveyed would lose trust in a company if it did not report an attack, and 22 percent if it paid a ransom.

All of the above may soon lead to a drop in the number of ransomware attacks, which does not bode well for ransomware operators and developers, who spend a lot of time and resources on developing and distributing malware.

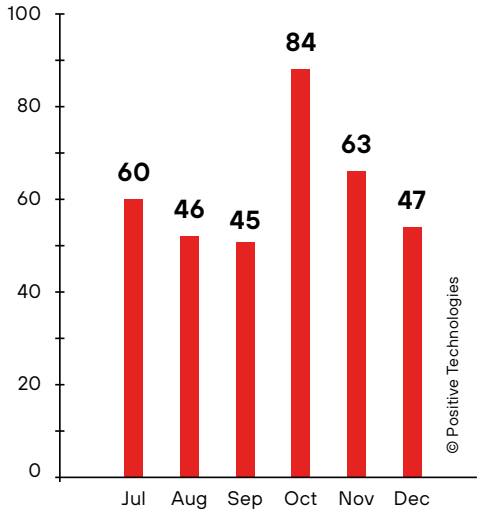


*Figure 9. Number of ransomware attacks (by month)*

The intelligence agencies' efforts to take down the REvil group sent a clear signal to cybercriminals that attacks on critical infrastructure and government institutions will not be tolerated. This had an impact on the distribution of sectors targeted by ransomware: for example, due to the greater oversight by law enforcement agencies, the share of attacks on government institutions fell by half against the previous quarter. Proof that ransomware operators have become wary of hacking into government systems comes from the AvosLocker and BlackByte attacks on a police station and a tax office, during which the intruders realized who they were dealing with and promptly offered a decryptor absolutely free of charge.

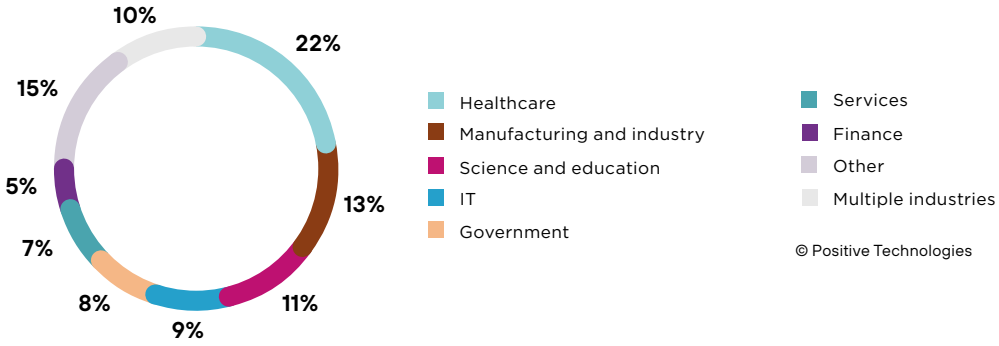


*Figure 10. Distribution of ransomware attacks by industry*

**Notable attacks in Q4**

The most active ransomware groups in Q4 were: LockBit 2.0, Conti, Hive, Pysa and PayOrGrief

**In the firing line**

In Q4, the U.S. National Rifle Association (NRA) joined the list of PayOrGrief victims. The attackers encrypted its network and threatened the organization with a major leak of confidential information if the ransom was not paid. After failed negotiations, the extortionists posted information stolen during the attack on their blog: documents about pro-NRA politicians and information about national grants and members' corporate insurance. Following publication of the stolen data, the attackers used Twitter bots to spread word of the hack.

### See no evil

In October, the Evil Corp group released the new ransomware program Macaw Locker, the latest rebranding of the Evil Corp ransomware family, as was the case with the DoppelPaymer ransomware that became PayOrGrief. The impact of the new ransomware was felt by Sinclair Broadcast Group, the second largest US broadcaster, and the tech giant Olympus: the former reported equipment malfunctions and difficulties getting on the air, while the second limited itself to stating that a full internal investigation was underway. It was not the first attack on Olympus in 2021. In September, the company was attacked by the BlackMatter ransomware.

### For love or money

Although ransomware developers and operators face immense pressure from law enforcement agencies and widespread blocking of ransomware topics in underground forums, they still find workarounds to continue their activities. Communication between cybercriminal groups plays a key role. The dedicated RAMP forum has become a haven for ransomware creators. The pooling of experience on such sites leads to the deployment of new attack methods: for example, the AvosLocker ransomware started booting target computers in safe mode to bypass security tools, as BlackMatter did before, and one forum user shared a Log4Shell exploit, which was later used by the LockBit 2.0 group. RAMP also helped to launch and find partners for the "next-generation ransomware" ALPHV (BlackCat), as it is described on the forum. Written from scratch in the Rust language, the ransomware compares favorably with competitors by virtue of its high performance, secure access to memory, decentralization of web resources, own data center for leaks, and, in the words of the developer, cross-platform capability.

# Botnets: their name is Legion

In Q4, the number of botnet-based attacks doubled in comparison with Q1, while DDoS attacks by "botnetized" devices posted record figures. To incorporate devices in their network, botnet operators attack vulnerable devices and deploy RATs from C2 servers. For example, researchers at Fortinet report that the operators of the MANGA botnet used the recently discovered RCE vulnerability CVE-2021-41653 in TP-Link devices to execute arbitrary code on vulnerable devices and download a RAT onto the device to carry out attacks.

> A botnet is a network of devices infected with malware that allows attackers to connect to and control devices remotely.

Botnets can incorporate a huge number of compromised devices that cybercriminals use for personal gain. One of the largest botnets to date is Meris, which includes approximately 250,000 devices ready to swing into action at the click of a mouse button and cause significant damage to victims. Although impressive, its resources cannot compete with its Chinese counterpart Pink. At its peak, this botnet, discovered in November 2019 by Qihoo 360's Netlab security team, consisted of 1.6 million devices, and it still remains a threat, commanding roughly 100,000 devices.

**You are many, I am one**

Devices infected with botnet operators' malware can be used to launch DDoS attacks. DDoS attacks aim to disrupt or completely shut down a service or resource by overloading it with a huge number of requests per unit of time (for example, a recent Mirai-based botnet attack had a capacity of about 2 Tbps).

A common ransomware method, DDoS can be used both in conjunction with other malware and on its own. Companies suffer enormous losses as a result of DDoS attacks: their sites or services become unavailable to users due to the sheer number of requests bombarding the server.

**The sound of silence**

Many organizations and individuals use VoIP telephony. So a sudden disruption of VoIP services can cause major inconvenience and losses to operators, which is what happened in October to Voipfone and in November to Telnyx. They were hit by massive DDoS attacks, resulting in widespread downtime of telephony services and frustration among users who relied on uninterrupted communication. It took Telnyx two days to resolve the issue, during which time they implemented anti-DDoS protection, while the attack on Voipfone left the company struggling for 72 hours to restore access.

October saw a whole series of companies hit by DDoS attacks (up to 256 Gbps) on mail services, causing email outages. The cybercriminals sent threatening messages with a ransom demand (around US$4,000) to halt the attacks.

### Second chance

The Emotet botnet is back, almost ten months after it was taken offline by law enforcement, and is busy recruiting another army of infected devices. To do so, its operators have teamed up with their long-standing partners, Trickbot and Conti. They decided to give their old acquaintance another chance, since it was Emotet that previously distributed the banking trojan and ransomware. Using malicious attachments in spam emails, Emotet is building an army of bots and recently has been using Cobalt Strike to gain immediate access to victims' networks. Such access will accelerate the attacks and may lead to another burst of ransomware activity.

# Supply chain: as strong as the weakest link

Throughout 2021, we saw a continuation of the trend to target software supply chains, which began in Q4 2020 with perhaps the most notorious supply chain incident: APT29's attack on SolarWinds. Back then, cybercriminals managed to gain remote access to thousands of organizations worldwide, including U.S. government agencies, using a zero-day vulnerability and software compromise through malicious updates.

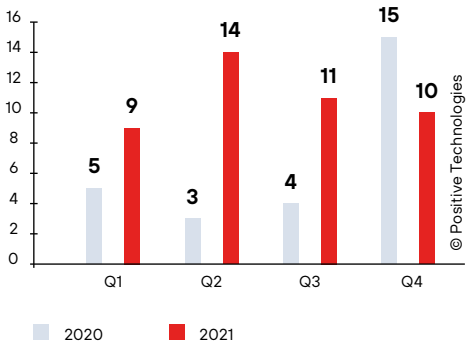


*Figure 11. Number of software supply chain attacks*

An Aqua Security report states that supply chain attacks have tripled since 2020 and highlights several vectors for such attacks, one of which is vulnerabilities in open source applications.

Cybercriminals pulled off such an attack in October, having injected malicious code open-source into the popular UA-Parser-JS library. Analysis of the embedded malicious code revealed the addition of malicious scripts that downloaded and executed binary files from a remote server, intended for both Linux and Windows systems. When run, the binaries downloaded XMRig, a Monero miner, and a credential stealer that stole passwords stored in the browser, as well as OS, mail, and instant messenger credentials. According to the developer, the library hack occurred after its NPM account was compromised, as confirmed by examining data from the developer's infected computer.

An additional threat is posed by the compromise of continuous integration and continuous delivery (CI/CD) tools. This can lead to source code disclosure, cybercriminal actions on the code during the build process, and the introduction of vulnerabilities, as in the case of GoCD. GoCD is an open source solution for automating continuous software delivery and integration. Some Fortune 500 companies use it. Researchers at SonarSource found a vulnerability in an update that removed support for the OAuth platform, making it possible for attackers to mimic a build agent and access features without authentication. The developers of the GoCD tool patched a critical vulnerability which, if exploited, could have led to extraction of tokens for confidential services, theft of source code, access to the original development environment, so on, potentially followed by a supply chain attack. Our study highlighted the importance of identifying and managing vulnerabilities.

# Deception all around

In Q4, 73 percent of attacks on individuals sought to steal confidential information, up 11 p.p. on the previous quarter. To achieve their goals, cybercriminals typically employed social engineering, while malware was used in 60 percent of attacks.

**Pocket spyware**

We noted a significant increase in the share of attacks on mobile devices—from 18 percent in Q1 to 29 percent in Q4, driven by the active distribution of banking trojans by cybercriminals.

In late October, Cleafy researchers discovered a new banking trojan for Android, which they named SharkBot. Once installed, the malware asks the user for access to Accessibility features, through which it gains almost complete control over the device. These permissions allow the trojan to mimic screen taps, log keystrokes to steal banking and other credentials, and intercept and hide text messages with authentication codes. But what makes this trojan special is its ability to automatically fill in the fields in banking apps and initiate the transfer of funds with little or no user input, bypassing multi-factor authentication.

At the time of detection, the trojan was not seen on Google Play. It was disguised as various apps, suggesting it was spread through third-party app stores and websites by tricking users.

**Hook, line, and sinker**

Cybercriminals are still using old phishing techniques to good effect, adapting them to the new realities. In particular, they are making hay from the digital money craze, which has attracted many crypto newbies.

Cofence researchers reported a new phishing campaign against CoinSpot users that asks them to confirm or cancel a withdrawal in an official-looking email, redirecting them to a phishing site. For added believability, the attackers include the transaction amount and the wallet address, and use email domains as close as possible to CoinSpot. Once on the phishing site, users are prompted for their credentials and a two-factor authentication code, after which the attackers take full control of the victim's account.

Two-stage attacks involving fake call centers continued in Q4. We already discussed such attacks in our Q3 report. In October, a Coinbase user fell victim to such an attack, having received a fake notification saying their account on the crypto platform was blocked and advising to contact the "support" team, whereupon they called the number in the email. During the brief conversation, the victim provided remote access to their account, and just ten minutes later the scammer increased the transfer limits and stole more than $11 million worth of cryptocurrency through a series of transfers to various accounts.

### Squid games

Hype is invariably exploited by attackers for criminal purposes. For instance, Proofpoint reports that the TA575 group made active use of the smash-hit show "Squid Game" as bait to spread the Dridex malware. The analysts detected a large number of phishing emails inviting targets to download a file to get early access to the new season or to register for a role as an extra in future seasons. The attached document contained a malicious macros that, when activated, downloaded and installed Dridex on the victim's device. The trojan can then steal the user's credentials and download other malware.

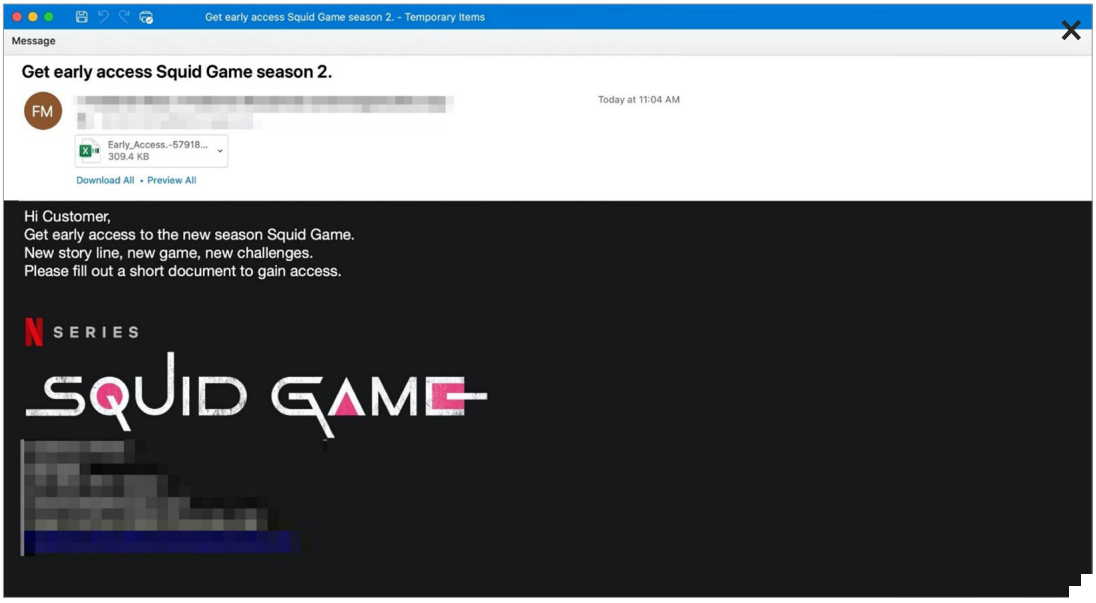


*Figure 12. TA575 phishing email (source: Proofpoint)*

# Current vulnerabilities in Q4

**A perfect storm**

In December, the whole world find out just how much one small detail can impact an entire system. Log4j is a Java library for logging application error events. It is widely used in both user and enterprise software products, including Apache, Elasticsearch, and even Minecraft. The Log4Shell vulnerability with the identifier CVE-2021-44228 was detected by Alibaba Cloud Security back in November. It was made public on December 9, receiving a maximum criticality score of 10.0, plus a PoC exploit was released for it.

The widespread use of the Log4j library, the public disclosure of PoC exploits, and the easy exploitation of the vulnerability meant that it soon started raining attacks: researchers from Check Point liken cybercriminals' exploitation of the Log4Shell vulnerability to a pandemic, since on December 10, the day after the vulnerability was made public, 10,000 attack attempts were recorded, rising to 40,000 on December 11; two days later the number of attack attempts exceeded 800,000 (an increase of 7,900% in just three days!).

The Log4Shell vulnerability immediately caught the eye of attackers: the Kinsing botnet, known primarily for crypto mining actively exploited the vulnerability to deliver malicious shell scripts to download backdoors and mining malware; the developers of the Conti ransomware added Log4Shell exploitation functionality to their programs; and Microsoft said in a report that attackers are using Log4Shell to deliver Cobalt Strike beacons. Nor did APT groups worldwide pass up the opportunity to exploit the vulnerability: for example, Aquatic Panda used it to attack Linux servers, and APT35 to target information systems in Israel.

**Virtuoso exploiters**

To achieve maximum impact, discretion, and speed, attackers use zero-day vulnerabilities—such attacks are difficult to detect and respond to quickly. These vulnerabilities are by no means accessible to all attackers, but APT groups often have the skills and resources to exploit them.

> In Q4, 14 percent of attacks were carried out by APT groups

In Q4, several APT groups actively exploited zero-day vulnerabilities in Zoho software, namely CVE-2021-44077 and CVE-2021-40539 in the ManageEngine ServiceDesk Plus and ManageEngine ADSelfService Plus products, respectively. These vulnerabilities provide remote code execution capabilities, and successful exploitation can lead to malware downloading.

A Palo Alto Networks report warned that the APT group TG-3390 was able to exploit the above-mentioned vulnerabilities to compromise the networks of at least 13 companies in the fields of tech, energy, healthcare, and finance using the Godzilla web shell and the NGLite backdoor to gain permanent access to networks, and the KdcSponge stealer to steal credentials.

# Ransomwarers switch to medicine

Medical institutions took top spot by number of attacks on organizations in Q4, accounting for 14 percent of all such attacks, which is 2 p.p. more than in the previous quarter. As before, clinics and hospitals remain the target of cybercriminals hungry for confidential information: 62 percent of cyberattacks resulted in a leak of personal or medical information (39% and 36%, respectively, of the total share of stolen data).

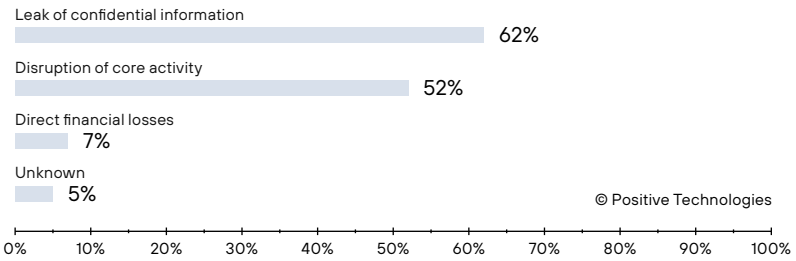


*Figure 13. Consequences of attacks on medical institutions*

Most malware attacks involved ransomware. One such attack severely impacted health authorities in the Canadian province of Newfoundland and Labrador. The Conti ransomware attack disrupted information systems, forcing regional healthcare centers to cancel chemotherapy appointments, X-rays, surgeries, and other services. Communications were also hit, with people reporting being unable to contact emergency services.

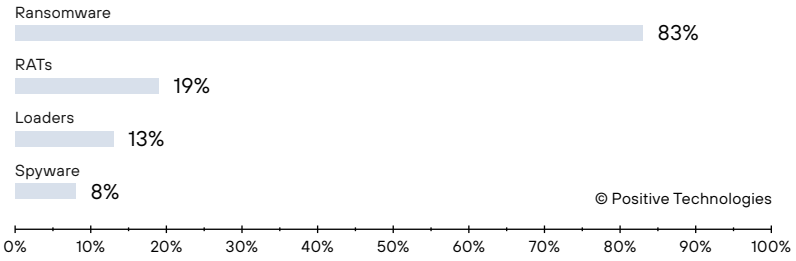


*Figure 14. Main types of malware in attacks on medical institutions (share of malware attacks)*

# Government agencies: hacks and spies

Government agencies had long suffered more than others from attacks, but in Q4 medical institutions were attacked 4 percent more often. This is partly because ransomware groups have shifted their attention to other industries due to increased law enforcement scrutiny of cyberattacks on government agencies. But the decline in the number of attacks on government agencies does not mean less severe consequences.

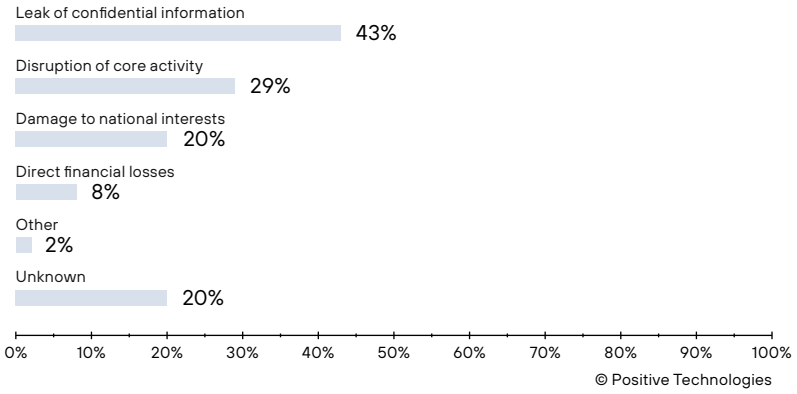


*Figure 15. Consequences of attacks on medical institutions*

### I know everything about you

In October, an unknown hacker carried out one of the most high-profile hacks of 2021 by gaining access to the Argentinian National Register of Persons (RENAPER), a government database, stealing the personal data of the country's entire population (around 45.3 million people), and putting it up for sale on the dark web. The stolen data included ID card photos and details.

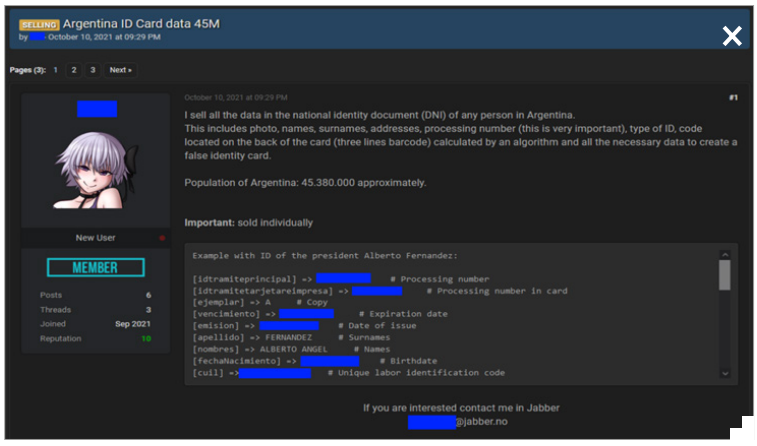


*Figure 16. The stolen database on sale (Source: The Record)*

## Festive bait

Malware and social engineering were used most often in Q4 attacks on government agencies (in 65% and 51% of attacks, respectively). APT groups whose goal is to spy on and steal sensitive data from government agencies employ a combination of the two.

PT ESC uncovered one such phishing campaign by the APT37 group. The attackers sent phishing emails to employees of a government agency containing New Year's greetings and an archive with a malicious attachment in the form of a Windows desktop screensaver. The purpose of the malicious attachment was to download an installation archive, unpack it, and run a file with a sequence of commands for installing "Screensaver Management Service" and the Konni RAT. This trojan, in turn, sent initial information about the compromised device and executed commands on the victim's device, calling the attackers' C2 server.

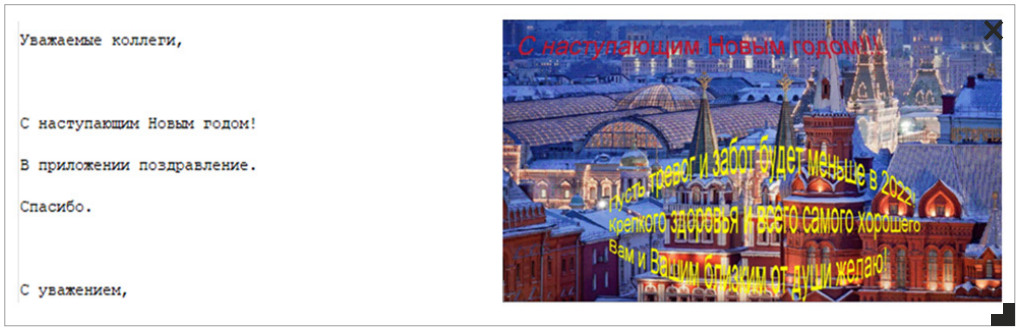


*Figure 17. Phishing email with malicious attachment*

## Trojan agenda

PT ESC detected ongoing attacks by the TA428 APT group in Mongolia. In one of its attacks on Mongolian government agencies, the group used a phishing document about a trilateral diplomatic meeting between Russia, Armenia, and Azerbaijan. The document was created using the Royal Road tool, which generates malicious RTF files that exploit the CVE-2018-0802 vulnerability, and equipped with a payload in the form of the nccTrojan RAT.

МОНГОЛ УЛСААС ОРОСЫН ХОЛБООНЫ УЛСАД
СУУГАА ЭЛЧИН САЙДЫН ЯАМ

ХЭВЛЭЛИЙН ОНЦЛОХ МЭДЭЭ

2021 оны 11 дүгээр сарын 23-ны өдөр | № /21 | Москва хот

**СОЧИ ХОТНОО 3 ТАЛТ УУЛЗАЛТ БОЛНО**

**Эхсурвалж:** https://tass.ru/politika/12999209

**Агуулга:** ОХУ-ын Ерөнхийлөгч В.В.Путин, Бүгд Найрамдах Азербайжан Улсын Ерөнхийлөгч И.Алиев, Бүгд Найрамдах Армени Улсын Ерөнхий сайд Н.Пашинян нарын гурван талт дээд хэмжээний уулзалт оросын талын санаачилгаар 2021 оны 11 дүгээр сарын 26-ны өдөр Сочи хотноо болох тухай Кремлын Хэвлэлийн албанаас мэдээлэв. Тус уулзалтыг 2020 оны 11 дүгээр сарын 9-ний өдөр Уулын Карабахд гал зогсоох гэрээнд гарыг үсэг зурсны нэг жилийн ойн хүрээнд зохион байгуулж байгаа бөгөөд хэлэлцээрийн хэрэгжилт болон цаашдын алхмуудыг хэлэлцэхээр төлөвлөж байгаа аж. Түүнчлэн гурван талт дээд хэмжээний уулзалтын хөтөлберт ОХУ-ын Ерөнхийлөгч В.В.Путин Бүгд Найрамдах Азербайжан Улсын Ерөнхийлөгч И.Алиев, Бүгд Найрамдах Армени Улсын Ерөнхий сайд Н.Пашиньян нартай тус тусад нь хоёр талын уулзалт хийхээр тусжээ.

**Лавлагаа:** Уулын Карабах орчмын мөргөлдөөн 2020 оны 9 дүгээр сарын 27-ны өдөр хурцадмал болж, тус бүс нутагт мөргөлдөөн эхэлсэн. Улмаар ОХУ-ын Ерөнхийлөгч В.В.Путин, Бүгд Найрамдах Азербайжан Улсын Ерөнхийлөгч И.Алиев, Бүгд Найрамдах Армени Улсын Ерөнхий сайд Н.Пашинян нар 2020 оны 11 дүгээр сарын 9-ний өдөр Хамтарсан мэдэгдэлд гарын үсэг зурснаар мөргөлдөөнтэй бүс дэх байлдааны ажиллагааг бүрэн зогсоох боломжтой болсон.

*Figure 18. Phishing document created by TA428*

# Industry: leaks and stoppages

In Q4, attacks on industrial companies accounted for nine percent of all attacks against organizations, placing this sector in third place by number of attacks. Malware was used in 90 percent of the attacks, the lion's share of which (56%) was ransomware.

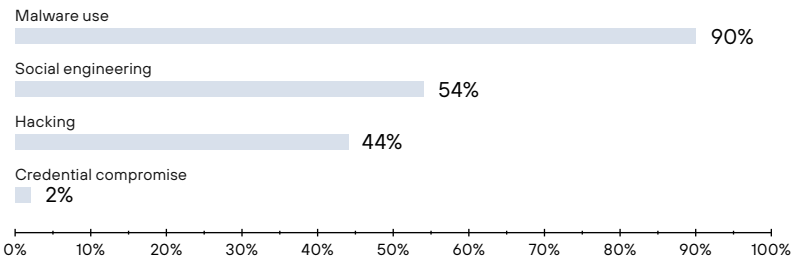


*Figure 19. Methods of attacks on industrial companies*

Industrial companies most often suffered disruption of core activities as a result of cyberattacks. For example, a ransomware attack on the automotive parts manufacturer Eberspächer Group affected virtually all of the company's information systems, paralyzing its activities and forcing it to send employees on paid leave during the clean-up.

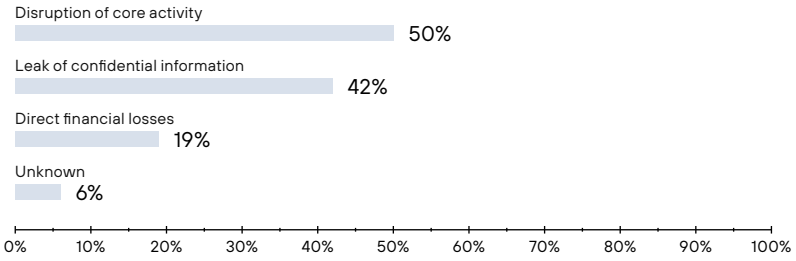


*Figure 20. Consequences of attacks on industrial companies*

In Q4, 42 percent of cyberattacks resulted in leaks of confidential information. Most notable were the attacks on Panasonic and Bosch. Cybercriminals stole the source code of Bosch iSite, a 5G wearable tech and IoT software platform, using a string of zero-day vulnerabilities in the SonarQube platform, and then posted it on a dark web forum. And in the case of Panasonic, malefactors gained unauthorized access to information about the company's tech and business partners, as well as employees' personal data.


*Figure 21. Cybercriminals posted the iSite source code on a forum*

# About the research

This report contains information on current global information security threats based on Positive Technologies' own expertise, investigation results, and reputable sources.

We estimate that most cyberattacks are not made public due to reputational risks. As a consequence, even companies specializing in incident investigation and analysis of hacker activity are unable to quantify the precise number of threats. Our research seeks 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.

This report considers each mass attack (for example, phishing emails sent to multiple addresses) as one incident, not several. For explanations of terms used in this report, please refer to the Positive Technologies glossary.