

Cybersecurity threatscape: Q3 2021



Contents

Summary	3
Statistics	4
Malware diversity	8
Attacks on Linux	9
When things don't work out from the start	10
Attacks on individuals	10
Ransomware rebuilding	12
Notable attacks in Q3	13
Familiar faces: return and rebranding	14
Nothing personal, just business	14
Achilles' heel: current vulnerabilities in Q3 2021	16
One click and it's game over	17
Vigilance is called for	18
Government agencies in the crosshairs	19
Healthcare is a treasure trove of data	21
The view from industry	22
About the research	24

Summary

Q3 2021 results:

- The number of attacks decreased by 4.8 percent against Q2 2021, mainly due to a drop in the number of ransomware attacks and the departure of some major players from the scene.
- The volume of targeted attacks on organizations changed insignificantly compared to the previous quarter: 77 percent in Q2 versus 75 percent in Q3.
- The share of attacks targeting individuals also changed little, rising from 12 percent last quarter to 14 percent this quarter. Sensitive information was leaked in 62 percent of cybercriminal attacks. In some cases, individuals fell victim to APT groups.
- The share of remote access tools (RAT) increased. In attacks on organizations, the figure grew to 36 percent among malware-based attacks (against 17% last quarter); in attacks on individuals, such malicious programs accounted for more than half of all malware used. Widespread use of loaders was also observed, in particular for expanding botnets.
- Cybercriminals are finding new ways to compromise Linux-based systems: the release of a Linux version of the Cobalt Strike Beacon Trojan is notable in this regard.
- As we anticipated, ransomwarers are rethinking their approach to Ransomware-as-a-Service (RaaS). Due to the lack of transparency of the RaaS model and the development of the market for exploits and access to companies, ransomware groups have begun to morph into more organized structures that seemingly adhere to the all-in-one concept.
- Among organizations, government agencies were most frequently attacked. Cybercriminal actions tended to result in leakage of sensitive information and disruption of state institutions. The main attack tool is ransomware, used in 46 percent of malware-based attacks.
- Medical institutions remain a primary target of cybercriminals. Sensitive data was leaked in 58 percent of attacks, and roughly half of all stolen information (45%) was medical.
- In the industrial sector, we note a sharp fall in the share of ransomware among malware-based attacks, from 80 to 32 percent. Meanwhile, APT groups have become more active in terms of cyberespionage; for example, attacks by APT31 and ChamelGang were detected.

To protect against cyberattacks, we advise that you follow our [guidelines](#) on personal and corporate cybersecurity. Given the nature of the attacks this quarter, we strongly recommend installing security updates in a timely manner and ensuring that vulnerability management processes are effective. 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 that analyze file behavior in a virtual environment and detect malicious activity.

Statistics

In Q3 2021, we saw a 4.8 percent decrease in the number of attacks against Q2, primarily due to the decline in ransomware activity. For the same reason, the share of attacks aimed at compromising corporate computers, servers, and network equipment fell from 87 to 75 percent. Most often, cybercriminals attacked government agencies, medical organizations, and industrial enterprises.

APT activity against individuals was observed (5% of attacks targeted individuals). This is due to the launch of numerous phishing and data-harvesting campaigns against employees of government agencies, industrial enterprises, and media organizations. 62 percent of attacks on individuals resulted in leakage of sensitive information: mostly credentials (41% of total stolen data) and personal data (21%).

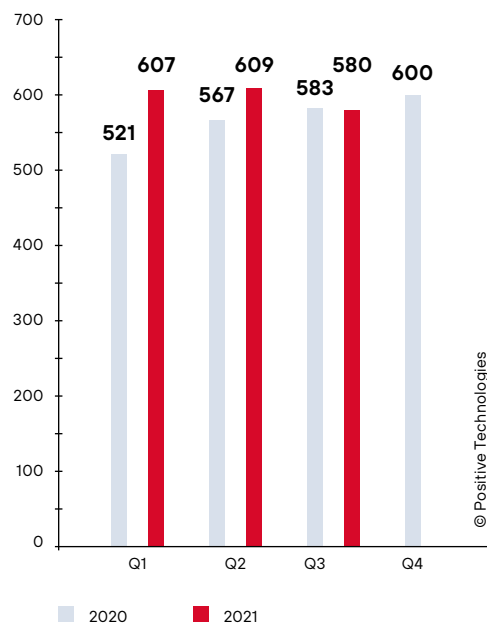


Figure 1. Number of incidents in 2020 and 2021 (by quarter)

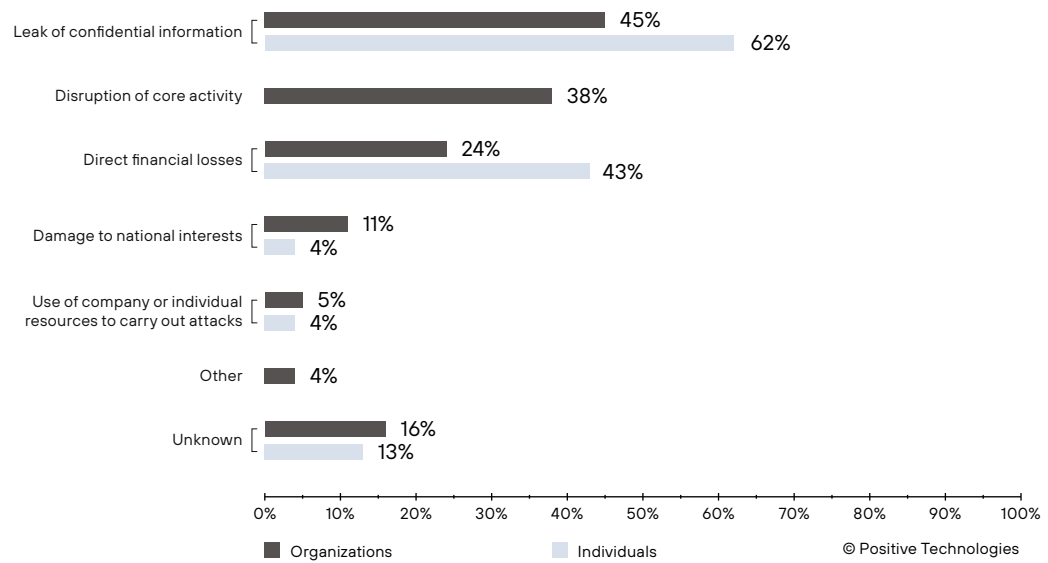


Figure 2. Attack consequences

77% of attacks were targeted

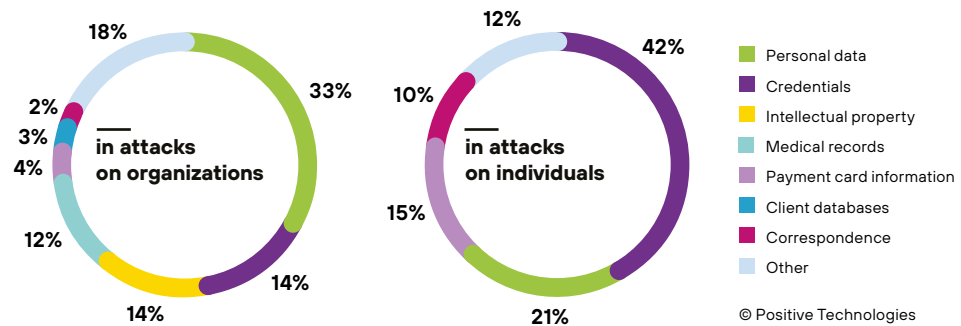


Figure 3. Types of data stolen

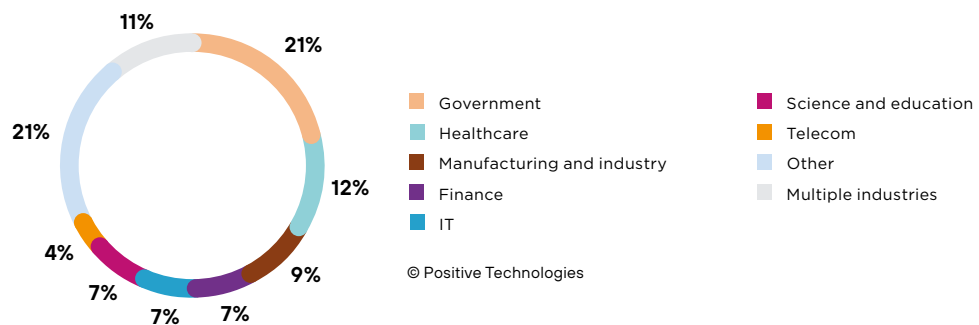


Figure 4. Victim categories among organizations

14% of attacks targeted individuals

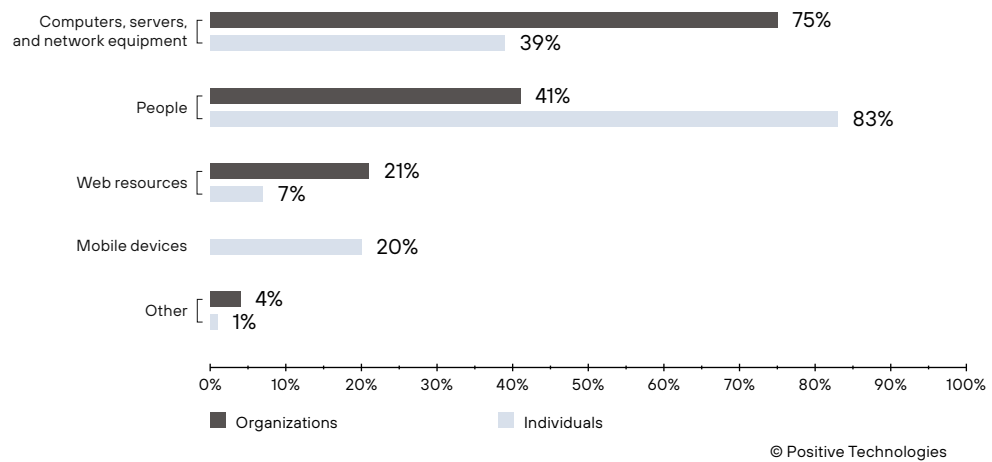


Figure 5. Attack targets

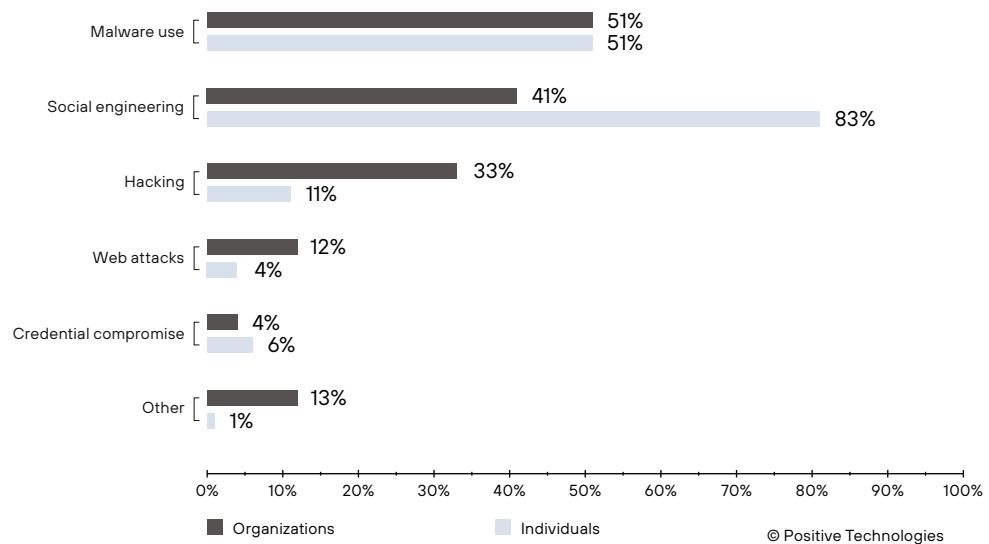


Figure 6. Attack methods (percentage of attacks)



Malware diversity

Compared to Q2 2021, the proportion of malware attacks targeting organizations decreased by 22 percentage points to 51 percent. Despite falling by 14 percentage points to 36 percent, ransomware attacks remain the most popular among cybercriminals; moreover, their pursuit of data led to an increase in the use of RAT, from 17 to 36 percent in attacks on organizations. We also note the upward trend in the use of loaders: attacks using loaders more than doubled in Q2 against Q1 and continued to grow in Q3 (15% and 21% in Q2, and 18% and 36% in Q3 in attacks on organizations and individuals, respectively).

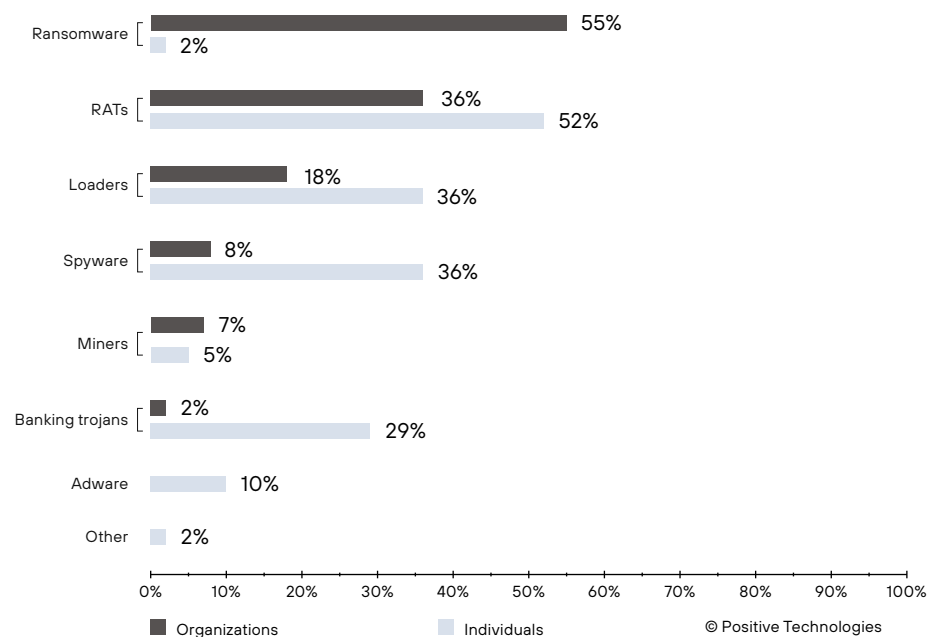


Figure 7. Types of malware (percentage of malware-related attacks)

In Q3, malware in attacks on organizations was distributed primarily via email (52%). One example is the spread of the Casbaneiro Trojan via malicious spam that passed through corporate mail filters by means of HTML smuggling.

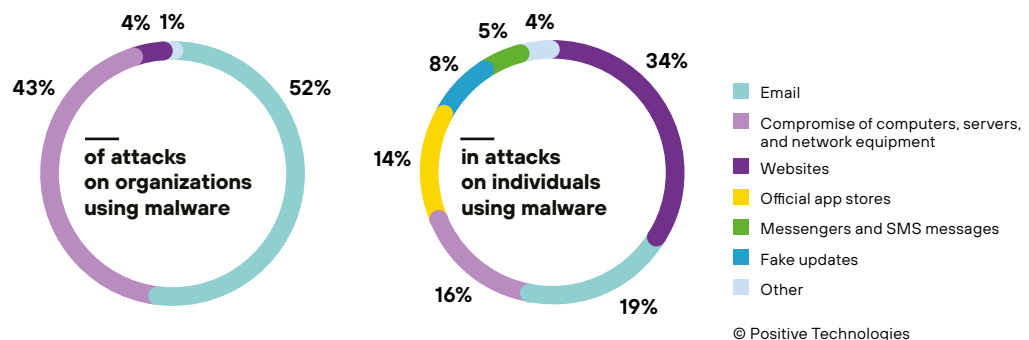


Figure 8. Methods used for malware distribution

Attacks on Linux

A beacon that leads you astray

It is widely believed that Linux systems are less vulnerable to attacks. This opinion is not surprising, since it is backed by some weighty arguments: 100 percent of the Top 500 supercomputers run under Linux; it is used by nearly 80 percent of web servers from the list of the million most-used domains worldwide; it is the operating system of choice in everything from smartwatches to spaceflight programs. But the more widespread a system becomes, the more cybercriminal attention it attracts, as we have seen throughout the year.

In August, researchers at Intezer discovered an actively used Linux version of the Cobalt Strike Beacon Trojan that had been created from scratch and was undetectable by antiviruses. The specimen was named Vermilion Strike. Attackers use Cobalt Strike Beacon to gain remote access to compromised systems, collect data, or load additional malware. The only drawback for them was that Cobalt Strike Beacon was Windows only. Vermilion Strike fixes this flaw. It uses the same configuration format as its Windows counterpart, communicates with Cobalt Strike C2 servers, has the same functionality, but does not use the Cobalt Strike source code.

Telemetry data indicates that Vermilion Strike has been used in attacks against government agencies, the industrial and telecommunications sectors, and IT companies worldwide since August 2021.

Disguised as a penguin

In 2016, Microsoft announced Windows Subsystem for Linux (WSL) for running a Linux image in a Windows environment and using, for example, the command line without starting a virtual machine. Although this innovation was welcomed by developers, it opened up new opportunities for attackers, which they exploited in Q3 2021.

Trying out new methods to stealthily compromise Windows machines, attackers used WSL to deliver payloads to victims' systems. Two variants of the malware were detected. One was packaged as an ELF executable for Debian using PyInstaller and relied on Python libraries to perform its task; the other used PowerShell and was packaged as an ELF for Windows.

When things don't work out from the start

We recently published a [study](#) on rootkits—programs (or sets of programs) for hiding malware in the system. However, there exists a type of malware even more dangerous than a rootkit, and it goes by the name of bootkit. The problem is that bootkits are loaded before the operating system, allowing an attacker to control the boot process and get maximum privileges.

This quarter, researchers discovered an [update to the FinFisher spyware Trojan](#), which is operated by Gamma Group. In its current version, the malware uses a UEFI bootkit that replaces Windows Boot Manager with a malicious copy. The researchers note that this approach allows attackers to install a bootkit without bypassing firmware security controls, but this infection vector is very rare due to its complex implementation.

Experts at Eclipsium identified a [Windows Platform Binary Table \(WPBT\) vulnerability](#) that affects all devices running Windows 8 or later, and can be used to install a bootkit. The main task of WPBT is to ensure that critical functions keep running. WPBT is known for allowing manufacturers to run their drivers and programs every time the operating system boots. The vulnerability, in turn, allows programs to run with an expired or revoked certificate.

Attacks on individuals

Since early 2021, we have seen an increase in the use of RAT and loaders in attacks on individuals. Compared to Q1, in Q3 2021 the use of RAT increased by 2.5 times, and loaders by 2.2 times.

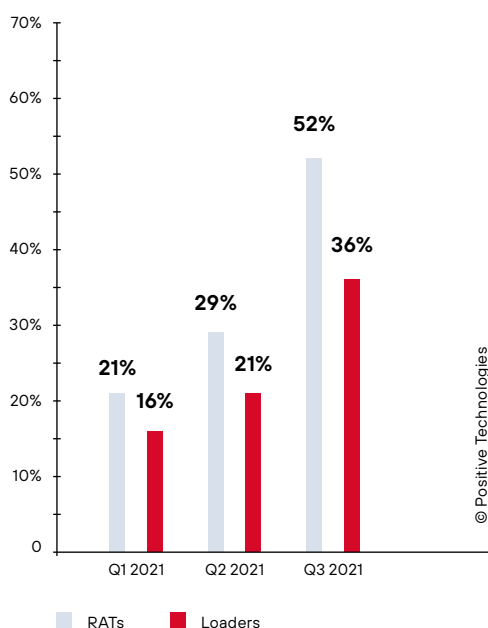


Figure 9. Use of RAT and loaders in attacks on individuals (share of malware-based attacks)

Trojan, but not the equine variety

Malware developers are constantly on the lookout for new ways to bypass security defenses and new tricks to infect victims' devices. An interesting new RAT specimen is the FatalRAT Trojan, discovered by AT&T Alien Labs. This Trojan is distributed via the Telegram messenger using malicious links posted on seemingly harmless resources or fake news channels. FatalRAT has a highly extensive feature set that includes:

- Logging keystrokes
- Intercepting messages
- Managing external connections and communication with the C&C server
- Making system changes without the owner's knowledge
- Downloading and running files
- Disabling security tools

FatalRAT is notable for its "cautious" behavior—the Trojan does not start its activity until sure that it is not in a virtual execution environment. All this makes FatalRAT a versatile tool for stealing user data.

Piecing together the mosaic

Of all the loaders detected in Q3 2021, MosaicLoader stands out. This loader spreads through advertising in search engines aimed at unscrupulous users looking for pirated versions of software. Researchers at Bitdefender draw attention to the concealment methods used by the loader:

- Imitation of file information similar to the original software
- Encryption of source code
- Fragmentary execution of the malware code in random order

When deployed on the victim's system, MosaicLoader downloads additional malware: cryptocurrency miners, cookie thieves, Remote Access Trojans (RATs), and backdoors. One type of malware delivered by MosaicLoader is the Glupteba Trojan. This in turn helped build the Meris botnet, which was behind the large-scale DDoS attack on Yandex in September.

Ransomware rebuilding

In Q3 of this year, we observed a rapid decline in the number of ransomware attacks compared to Q2. Ransomware attacks peaked in April, when 120 were recorded. September recorded 45 attacks, down 63 percent from the April peak. This is due to the deactivation of some major ransomware groups and the increased attention to the issue of ransomware attacks (following some high-profile incidents) by law enforcement agencies. The U.S. Treasury Department announced sanctions against cryptocurrency exchanges that facilitate ransomware operations. In September, these measures were taken against a number of cryptocurrency exchanges involved in cybercriminal transactions.

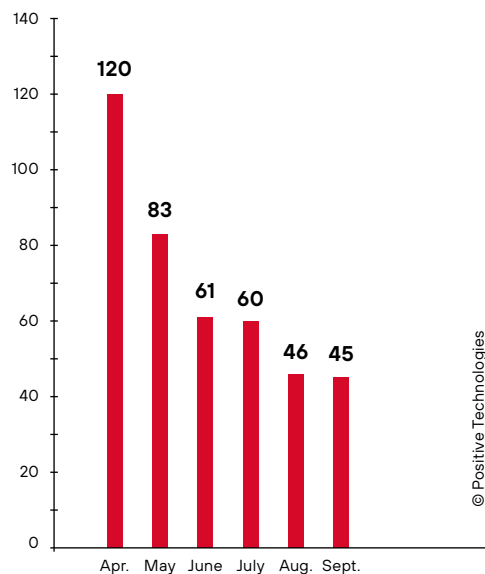


Figure 10. Number of ransomware attacks (by month)

Most often, ransomware encryptors attack government, medical, scientific, and educational institutions, as well as industrial enterprises.

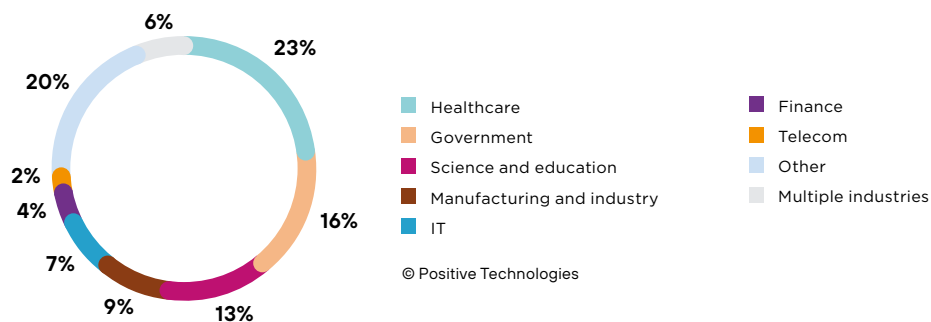


Figure 11. Ransomware attacks by industry

Notable attacks in Q3

The following ransomware encryptors were the most common in Q3 2021:

- REvil¹
- LockBit 2.0
- Conti
- Hive
- AvosLocker

The biggest splash in Q3 2021 was caused by the REvil attack on Kaseya on July 2, which affected more than 1,500 client organizations that used Kaseya VSA to administer their IT infrastructure. Having discovered a zero-day vulnerability in Kaseya VSA, REvil was able to bypass authentication in the VSA web interface and deploy ransomware on all active servers. As soon as the attackers gained control of VSA, they denied access to system administrators and began distributing the malicious VSA Agent Hot-fix update to all connected agents. The update made it possible to bypass Windows Defender and encrypt victims' systems. REvil then demanded \$70 million for a universal decryptor to decrypt the affected data. The ransom was soon reduced to \$50 million, but on July 13 REvil's servers suddenly shut down, leaving victims without a decryptor. However, on July 22 Kaseya received a universal decryptor for all REvil victims from a "trusted third party."

Two big-name companies were simultaneously attacked by LockBit 2.0 in Q3. The first was Accenture. Attackers gained access to the consulting giant's corporate systems, deployed their ransomware, stole 6 TB of sensitive data, and requested a \$50 million ransom, which, it later transpired, they did not receive; they then posted all the stolen information on their onion blog. During its campaign to expand its affiliate program, LockBit actively recruited insiders able to provide access to victims' corporate systems. According to the cybercriminals themselves, it was one of these insiders who helped them into Accenture's systems. The second company to be attacked by LockBit 2.0 was Bangkok Airlines. The attack resulted in the theft of around 200 GB of sensitive information, including passengers' passport data, flight history, and bank card details. The airline refused to enter into negotiations, and its data suffered the same fate as Accenture's.

Some cybercriminals, such as LockBit 2.0, claim not to target medical and educational institutions. But for others, money is more important than decency and their own reputation; this proved to be the case with the Hive group, which in August attacked several hospitals and extracted ransoms from them. Fortunately, no patients were harmed, but we know full well that cyberattacks can have human costs.

¹ Its servers were unexpectedly shut down after an attack on the software company Kaseya, and at the time of writing its infrastructure was in FBI hands.

Familiar faces: return and rebranding

Q3 is memorable for the return of some old players to the fold and the rebranding of active ransomware groups. The ongoing rebranding seems to have been prompted by the advisory issued by the U.S. Treasury's Office of Foreign Assets Control (OFAC) to impose sanctions on those who pay ransoms to cybercriminals, coupled with the close collaboration between the intelligence services and the Cybersecurity and Infrastructure Security Agency (CISA) to clamp down on ransomwarers.

Grief knows no bounds

As reported by Zscaler, one of the rebranders was the DoppelPaymer group, which almost completely shut down its operations on May 7, 2021, just after the high-profile REvil attack on Colonial Pipeline. Before the rebranding, DoppelPaymer was considered by many researchers as a member the Evil Corp syndicate, but, in light of recent events, the syndicate attracted too much attention, and it was decided to rename the ransomware PayOrGrief. The researchers discovered that the PayOrGrief executable file is compiled with DoppelPaymer code, uses identical encryption algorithms, and redirects victims to the DoppelPaymer ransom portal, clearly hinting at a direct link between the two groups.

Black is always in fashion

In July, researchers at Recorded Future found a new ransomware group called BlackMatter, which combines the most potent features of the defunct DarkSide and REvil. The cybercriminals bought access to various corporate systems on the Excile forum. Fabian Wosar confirmed on Twitter that BlackMatter uses the same unique encryption methods as did the DarkSide group in its attacks.

Two is better than one

Q3 2021 saw the return of LockBit 2.0—with some improvements. Having been inactive for almost a year, it is now very popular among cybercriminals (the first spike in activity was spotted from July 1 to July 15 by researchers at TrendMicro). Attackers are also actively recruiting affiliates, attracting insiders and qualified pentesters, posting offers in ransom notes.

Nothing personal, just business

To the face and behind the back

While analyzing the REvil ransomware, researchers at Advanced Intelligence discovered that the developers had inserted a backdoor, allowing them to secretly contact the victim and take the whole ransom for themselves.

REvil operates according to the RaaS scheme. This means that the developers only create and modify the malware and payment sites, while their affiliates do the hacking of networks and deliver the malware to compromised systems. On payment of a ransom, most often the money is distributed as follows: 70–80 percent to affiliates, the remainder to developers.

But in this case, the developers decided to play dirty. During the negotiation process, they opened a new chat with affiliates where they posed as a victim who refused to pay up, all the while negotiating with the real victim with a view to pocketing the entire ransom for themselves. Rumors about this flooded the pages of hacker forums for a long time, and were finally confirmed when the ransomware encryptor was reverse-engineered and a universal decryptor was released after the REvil attacks. In essence, the developers' main private key was both "insurance" against rogue affiliates and the key for decrypting any victim data.

Such sneakiness undermines the developers' reputation, and their sudden disappearance is very similar to an exit scam—a fraudulent technique whereby cybercriminals stop their activities, while still receiving money from clients or affiliates. The REvil case calls into question the principle of transparency between developers and affiliates—a fundamental aspect of the RaaS scheme.

Promising the moon

Another example of RaaS-based duplicity comes from the Conti ransomware operators. They offer the same scheme as REvil: 70–80 percent of the ransom goes to affiliates who hack networks and encrypt devices, and the remaining 20–30 percent goes to developers. However, in reality, one of the affiliates received only \$1500 for its efforts, a tiny amount given the size of the payouts by Conti victims.

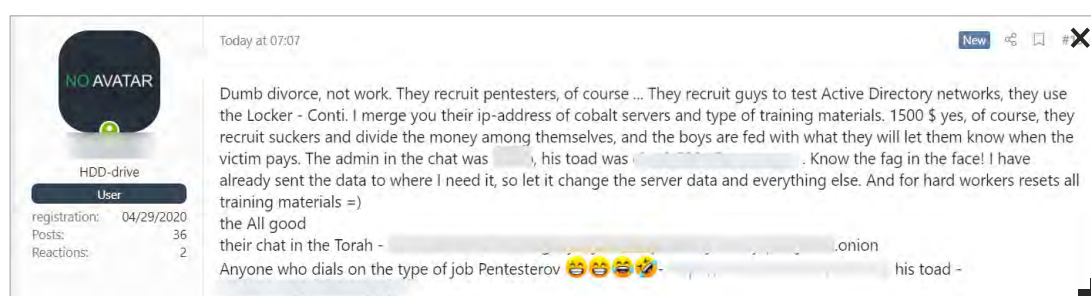


Figure 12. Forum post from a disgruntled affiliate

In response, the affiliate posted information about the Conti operators on a hacker forum, including full training materials for conducting ransomware attacks. In addition, the former affiliate posted screenshots of the IP addresses of the Cobalt Strike C2 servers used in the attacks.

This leak illustrates the risks of the RaaS scheme from developers' point of view, because a disgruntled or unscrupulous affiliate can reveal carefully collected, structured, and confidential attack-related information in one go.

Last quarter, we noted that the next move for ransomwarers could be to abandon the RaaS model in its current form. It is much safer for ransomware operators to hire people to deliver malware and search for vulnerabilities as "in-house" employees. It is safer for both parties through introducing a more organized and efficient form of interaction closer to the all-in-one concept. An additional driver of this approach is the growing sales market for exploits and access to companies that we wrote about in our report. Moving in that direction is the LockBit 2.0 group, which runs a closed affiliate program with carefully selected candidates and works with regular partners, buying access to various companies.

Achilles' heel: current vulnerabilities in Q3 2021

The number of attacks on Microsoft Exchange servers exploiting ProxyLogon vulnerabilities is not falling, despite Microsoft having released patches for them. For example, the EmissaryPanda APT group was observed exploiting a ProxyLogon vulnerability in an attack on a pentesting company.

Another current vulnerability in Q3 worthy of such designation is PrintNightmare, which was exploited by the Vice Society ransomware for distribution across the victim's network. The vulnerability affects the spoolsv.exe print spooler, a Windows service that acts as an interface between the operating system and applications and local or network printers. This is not the first time that a print spooler vulnerability has been exploited. For example, it was used by the Stuxnet worm in 2010.

Another Q3 group of vulnerabilities is ProxyShell, which consists of three vulnerabilities: CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207. They can be used to run arbitrary code on Microsoft Exchange servers without authentication.

Researchers at DEVCORE detailed these vulnerabilities at the recent BlackHat conference, where a PoC exploit for ProxyShell was also unveiled. Following the publication of the PoC exploit, researchers at ISC SANS found that more than 30,000 Exchange servers were vulnerable to attack, and just a week later some researchers stated that a ProxyShell vulnerability had been exploited to deliver the Lockfile ransomware and deploy backdoors. ProxyShell exploitation was also reported by PT ESC in its study of the ChamelGang APT group, which used a ProxyShell vulnerability to penetrate the infrastructure of a Russian aviation firm.

Assets / Vulnerability Passport

7.9 Remote code execution | [CVE-2021-34473](#)

Remotely There is a fix

basic information

Danger **High level**

Assets **7**

Vulnerabilities **5** **2** **0**

Description

A vulnerability in Microsoft Exchange could allow remote attackers to execute arbitrary code and interfere with the system.

How to fix

Use the manufacturer's recommendations:
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473>

Assessment by CVSS v3

General **7.9**

Basic **9.1 - AV: N / AC: L / PR: N / UI: N / S: U / C: H / I: H / A...**

Temporary **7.9 - E: U / RL: O / RC: C**

Additional Information

Date of publication Jul 13, 03:00

Identifier [CVE-2021-34473](#)

Pentest check Not applicable

Vulnerable components Microsoft Exchange

Assets with such vulnerabilities

Significance	Vulnerabilities		
High	4	2	0
Average	No vulnerabilities found		
Low	1	0	0
Unspecified	No vulnerabilities found		

Groups with such vulnerabilities

Group	Vulnerabilities		
ActiveDirectory	1	0	0
All Windows Hosts	5	2	0
CompanyName	5	2	0

Show more 4

Database identifiers

Identifier	Vulnerabilities		
CVE-2021-34473	5	2	0
MP8ID: MP8ID-418330	5	2	0

Figure 13. Detecting the CVE-2021-34473 vulnerability

One click and it's game over

Another dangerous vulnerability exploited by cybercriminals in Q3 was [CVE-2021-40444](#) in MSHTML, the Internet Explorer engine, for remote execution of malicious code on the victim's computer. This vulnerability also affects MS Word and MS PowerPoint, which access MS IE when handling web content.

To exploit the vulnerability, attackers create a special Microsoft Office document and deliver it to the victim in various ways (most commonly by email). The document contains a malicious ActiveX control that, when opened, gets processed by the IE engine. When the document is opened, Microsoft Office downloads a malicious script from the embedded link and runs it using MSHTML. The script can then use ActiveX controls to perform malicious actions on the victim's computer.

PT Expert Security Center revealed that APT groups have been exploiting this vulnerability in attacks on Russian government agencies, as well as aerospace and IT companies. For example, this is how the Winnti APT group delivered its Bisonal backdoor. Researchers at RiskIQ believe that the [Wizard Spider](#) ransomware syndicate exploited the vulnerability to deliver and deploy its own BazaLoader, as well as Cobalt Strike Beacon and [Conti \(Ryuk\)](#) payloads.


X

УВЕДОМЛЕНИЕ, КАСАЮЩЕЕСЯ НЕЗАКОННЫХ ПРЕСТУПЛЕНИЙ (2021.9.14.)

Пожалуйста, заполните форму ниже и отправьте ее на официальный адрес электронной почты Министерства внутренних дел или ответьте на это письмо, чтобы проверить свою активность.

Имя	
День Рождения	
Банковский счет	
Номер кредитной карты	
Эл. адрес	
Номер телефона	
Номер мобильного	
Женатый	Да / Нет
Количество Детей	
Дата Приема На Работу	

Мы принимаем документ о вашей деятельности в течение 7 дней после отправки этого письма.



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ

СПРАВОЧНЫЙ ТЕЛЕФОН-АВТОИНФОРМАТОР: 8 (495) 667-04-02

Figure 14. Phishing document with malicious content (containing details of the Russian Ministry of Internal Affairs)

Vigilance is called for

The number of attacks on individuals using social engineering has increased significantly: if in Q3 2020 the share of such attacks was 67 percent, this quarter it jumped to 83 percent. Cybercriminals do not stand still and are constantly refining their scam techniques.

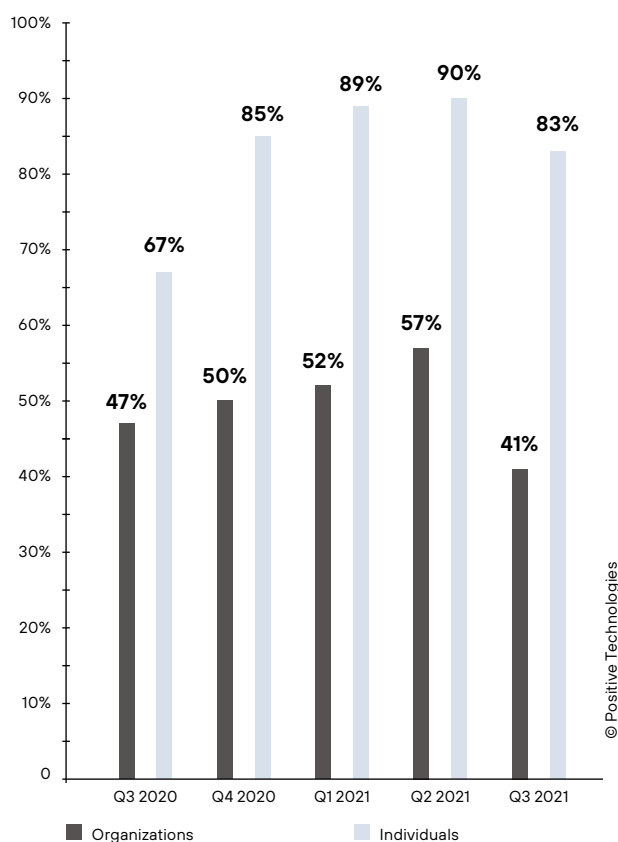


Figure 15. Attacks using social engineering

You called, your fault

In July 2021, Microsoft 365 Defender Threat Intelligence Team identified a new campaign to distribute BazaLoader, Conti (Ryuk), and even Cobalt Strike Beacon payloads, and named it BazaCall. Victims receive phishing emails notifying them that they will soon be charged for a subscription that is coming to the end of the trial period. To cancel the "subscription," the victim is asked to call a specific number.

Besides phishing, this campaign employs an uncommon technique: fake call centers. Victims that swallow the bait and make the call are connected to someone posing as a call center operator, who gives instructions to download an Excel file supposedly for canceling the subscription. When the file is opened and the macro activated, BazaLoader is loaded onto the device.

The difference with this method is that the phishing emails do not contain malicious attachments or links that the user can view or open. The lack of tell-tale attributes complicates detection by security solutions, and users are not always aware of such non-standard social engineering methods.

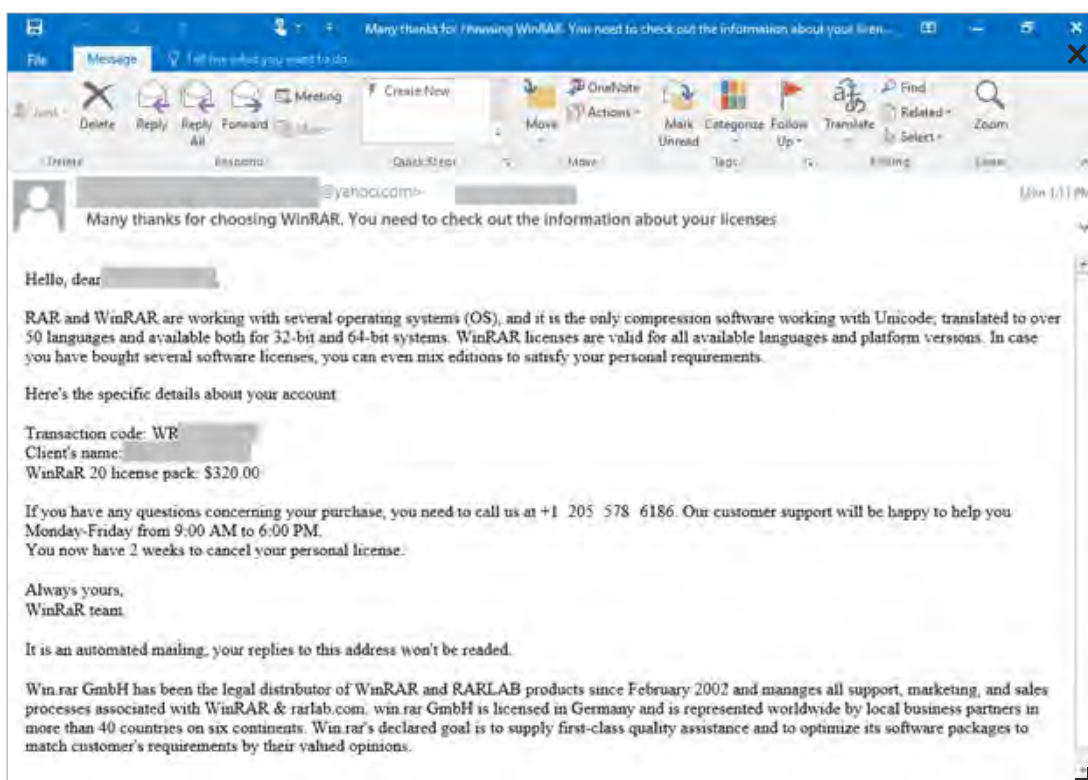


Figure 16. Example of a phishing email

Government agencies in the crosshairs

Government agencies top the leaderboard by number of attacks on organizations, although their share fell from 20 percent in Q2 to 18 percent.

Most of the attacks relied on malware (45%) and social engineering (42%). Ransomware encryptors played first fiddle in malware attacks (46% of cases). The most serious attacks on government agencies in Q3 were carried out by groups such as PayOrGrief, which attacked the systems of the Greek city of Thessaloniki, paralyzing e-government, tax and transport systems, and Lockbit 2.0, which attacked the Italian region of Lazio, disrupting almost the entire IT infrastructure, including online medical services. The second most common vector was RAT (44% of malware-based attacks), used, for example, by the ChamelGang and MustangPanda APT groups for espionage purposes.

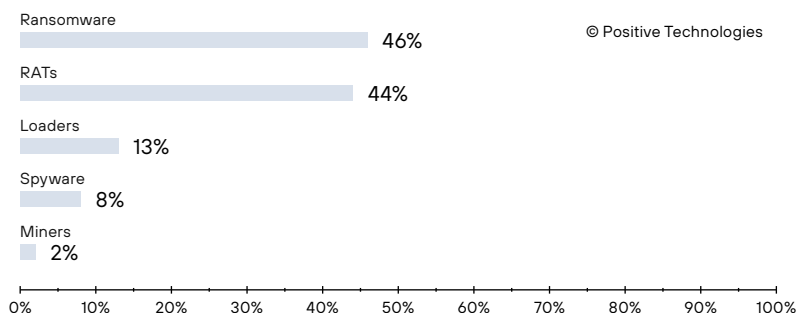


Figure 17. Types of malware in attacks on government agencies (share of malware-based attacks)

Most often, attacks caused leakage of sensitive information and disrupted the activities of state institutions (both these consequences were reported in 39% of cases). This in turn is indirect confirmation that government agencies have become the most common targets of ransomware and APT groups: the former seeks to disrupt information and infrastructure access for ransom purposes; the latter to carry out cyberespionage and extract confidential information.

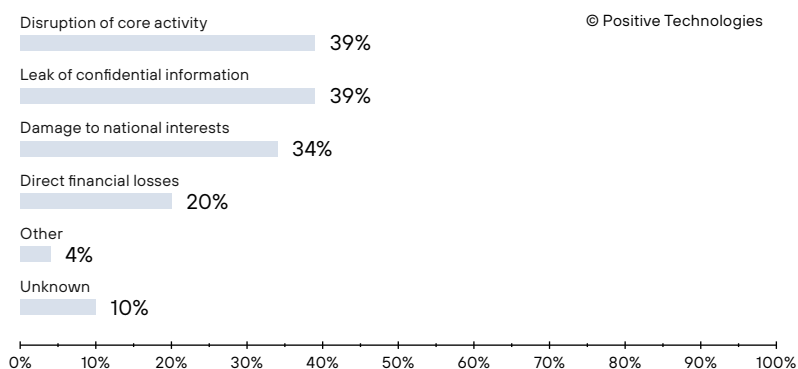


Figure 18. Attack consequences (share of attacks on government agencies)

Healthcare is a treasure trove of data

Medical institutions ranked second by number of attacks on organizations in Q3 2021. Healthcare accounted for 11 percent of the total number of attacks, up slightly on the previous quarter (10%). Clinics and hospitals attract cybercriminals: due to the COVID-19 pandemic, they have accumulated large volumes of sensitive data.

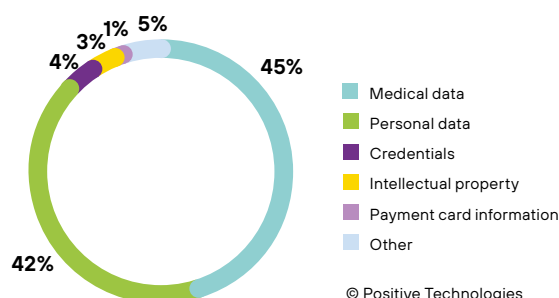


Figure 19. Types of stolen data in attacks on medical institutions

As such, the most common consequence of attacks on medical institutions was leakage of confidential information (58% of cases). For instance, cybercriminals used phishing to hijack work accounts of healthcare employees and steal data, as in the [attack on UC San Diego Health](#).

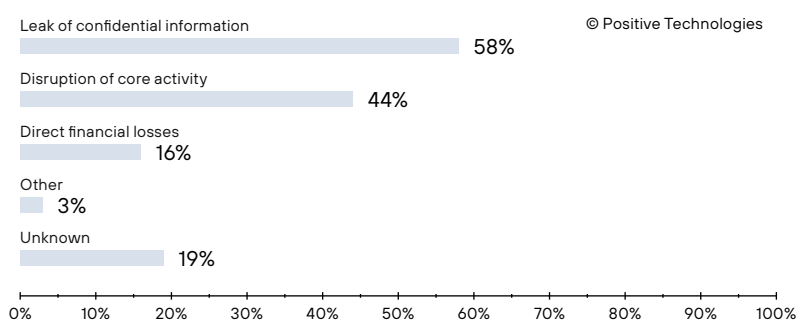


Figure 20. Consequences of attacks on medical institutions

Disruptions to core activity were most often caused by ransomware attacks (reported in 44% of cases). The largest ransomware attack on a medical institution is perhaps the one on [Memorial Health System by the Hive group](#). The attackers caused the IT infrastructure of three hospitals to collapse, disrupted scheduled operations and patient admissions, stole 1.5 TB of personal information, including patient data, and subsequently received a ransom payout of \$1.8 million for decryption and non-publication of the stolen information.

The view from industry

Industry lies in third place by number of attacks on organizations in Q3 2021 (8% of all attacks). In Q3, we again observed an increase in the share of hacking (45%) and malware (79%).

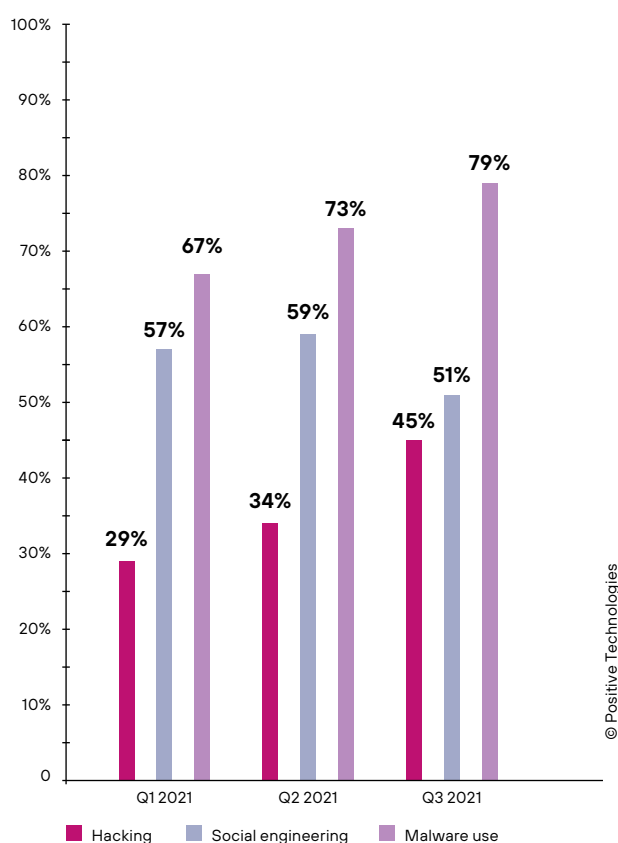


Figure 21. Share of methods used in attacks on industry

RAT was used in 51 percent of attacks on industry. Such attacks generally aim to gain access to systems and steal sensitive data; in some cases, this involves long-term entrenchment in the system and cyberespionage. In July 2021, the APT group Aggah used WarzoneRAT in attacks on manufacturing companies in Asia. In addition, PT ESC detected activity by the APT group APT31, which used the DropAES Trojan in a cyberespionage campaign against industrial companies in Russia, the U.S., Canada, and other countries. Compared to the previous quarter of this year, the share of attacks using loaders to deliver malware to compromised systems rose significantly (by 37 percentage points).

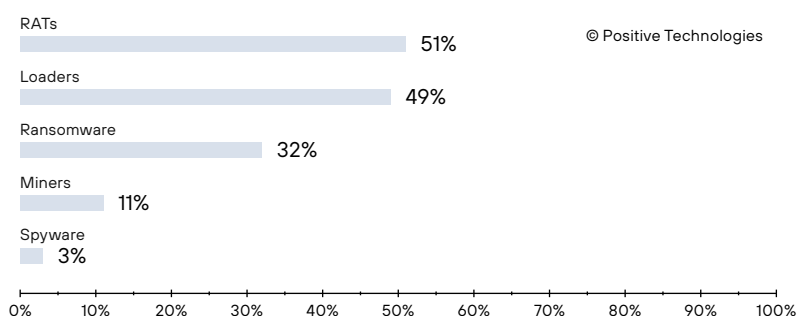


Figure 22. Main types of malware in attacks on industrial companies (share of malware-based attacks)

We noticed a significant decrease in the share of ransomware on the industry: down to 32 percent this quarter versus 80 percent in the previous one. We ascribe this to the excessive attention that ransomware attacks operators received from law enforcement agencies and security researchers last quarter. This is reflected in the statistics on the impact of attacks on industry.

Most often, attacks on industrial companies resulted in leakage of sensitive information (66%), which is explained by the large number of cyberespionage campaigns carried out by APT groups against industrial companies.

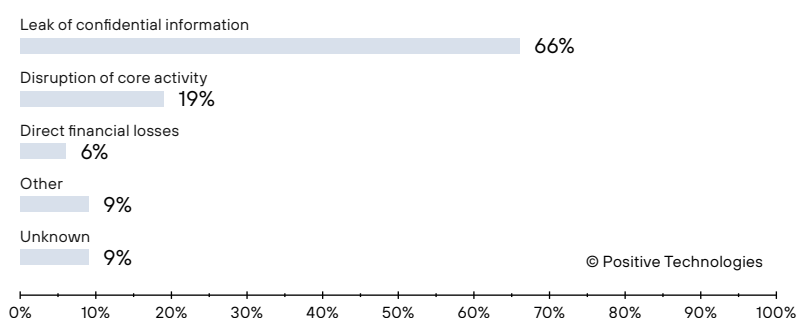


Figure 23. Consequences of attacks on industrial companies

Industrial companies are attacked not only through corporate networks, but through employees and their personal social media accounts. Proofpoint published an expert [report](#) about a long-running operation on Facebook. The APT group [TortoiseShell](#) set up an account to mimic a real person (an aerobics instructor) in order to connect and build a rapport with company representatives from the aviation and defense sectors. And it [worked](#)!

Using the fake account, the attackers made contact with an employee of a subsidiary of an aerospace defense contractor back in 2019, and only in 2021 did they send a link to OneDrive, from where an archived document (a survey on dietary habits during the pandemic) containing a malicious macro was downloaded. Once the content was enabled, the [Lempo](#) stealer was installed on the victim's computer, which harvested information about the device, users, and security tools installed.

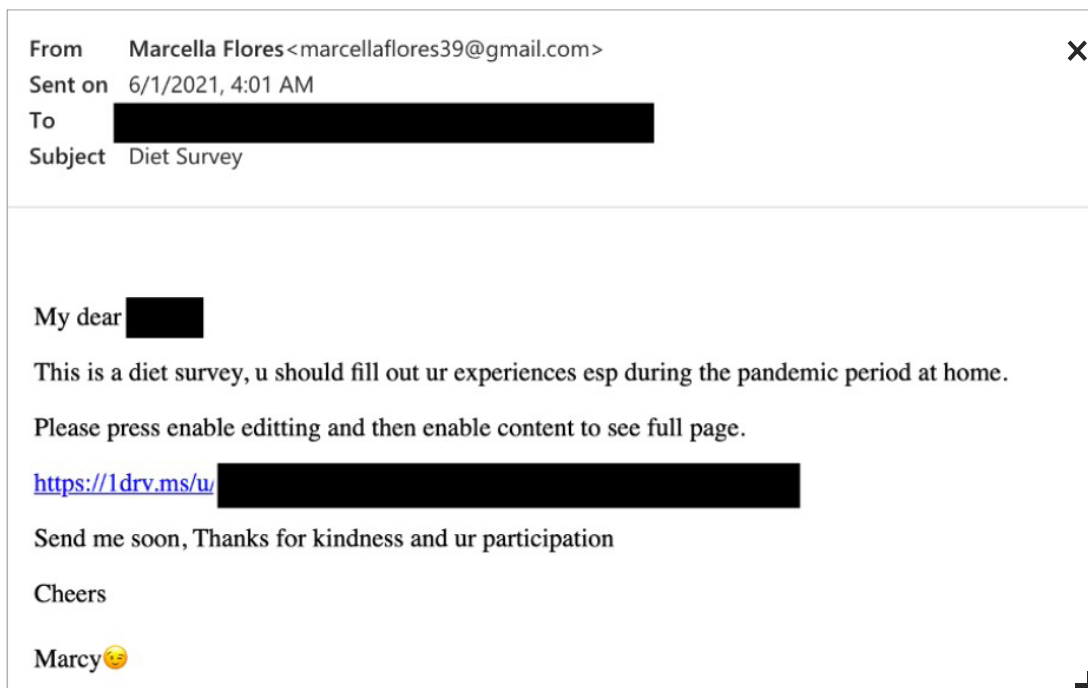


Figure 24. Email with a link to a malicious document (from the Proofpoint [report](#))

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 the terms used in the report, please refer to the [glossary on the Positive Technologies site](#).