Cybersecurity threatscape Q3 2022

Positive Technologies

ptsecurity.com

Contents

Summary

Q3 2022 highlights:

- The number of attacks increased by 10% compared to Q2 2022 and by a third compared to Q3 2021.
- Attacks on individuals accounted for 18%, with 46% of them being spyware attacks, which reflects the continuing upward trend.
- There has been no significant change in malware types employed in attacks: ransomware remains number one in attacks on organizations. The use of malware targeting Linux grew by 18 percentage points versus Q2. New sophisticated attack frameworks emerged.
- Ransomware activity remained at the level of the previous quarter. In most cases, attackers penetrated corporate systems by compromising RDP connections, exploiting vulnerabilities, or using initial access broker services. Ransomware groups showed increased interest in energy companies, scientific establishments, and educational institutions.
- Attackers partially shifted from disrupting core operations to stealing sensitive information, mostly credentials. Credentials increased by 8 percentage points compared to Q2 2022 and accounted for 17% of data stolen in attacks on organizations.
- Phishing kits are growing more popular in attacks aimed at collecting credentials. Such kits include preconfigured phishing pages, data entry forms, scripts for sending messages to victims, and scripts for sending stolen data to attackers. The phishing-as-a-service model is proliferating on the web. Cybercriminals create platforms to distribute phishing kits, enabling even relatively unskilled scammers to launch phishing attacks.
- Due to the widespread use of multifactor authentication, criminals are turning to reverse proxy servers to bypass it.
- Q3 saw mass attacks on web resources: attackers used common vulnerabilities in popular CMSs to compromise websites, deployed web skimmers, and used phishing kits to attack users.

To protect against cyberattacks, we first and foremost recommend following our general guidelines on personal and corporate cybersecurity. We advise keeping all software up-to-date and installing security updates. Given the intensified use of phishing kits and mass attacks involving social engineering, you should also be more careful when receiving emails, especially if their senders are not trusted persons. Organizations need to swiftly inform their employees about new phishing schemes, as well as tactics and techniques used by fraudsters. When buying online or making online payments, make sure that you are using a legitimate platform. Companies can strengthen the security of their web resources using modern security tools such as web application firewalls (WAFs). To prevent malware infection, we recommend using sandboxes that analyze file behavior in a virtual environment and detect malicious activity.

Statistics

In Q3 2022, the number of cyberattacks increased by a third compared to the same period in 2021, and by 10% compared to Q2 2022. Analysts attribute this growth to the ongoing confrontation in cyberspace, hacktivist activity, emergence of new ransomware, and evolution of existing malware. The share of attacks on computers, servers, and network equipment of organizations increased by 6 percentage points as a result of ransomware activity. In addition, the number of mass attacks increased by 4% compared to the previous quarter.

At the beginning of the second half of 2022, cybercriminals shifted their focus from disrupting core operations of organizations to stealing credentials, developing phishing tools, and refining social engineering techniques

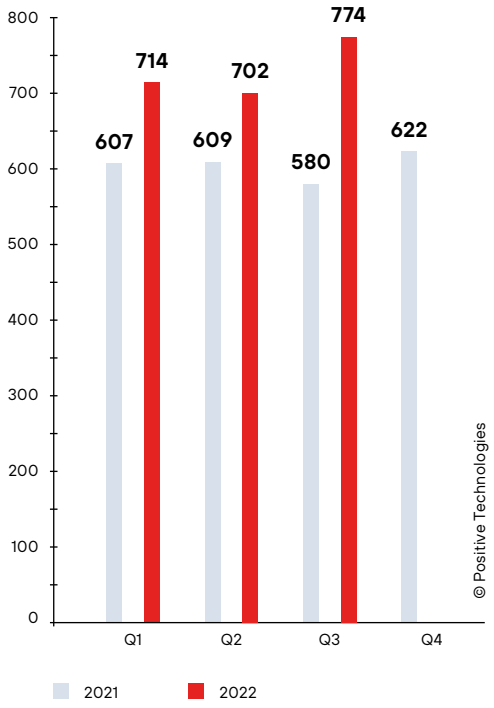

Figure 1. Number of attacks in 2021 and 2022 (by quarter)

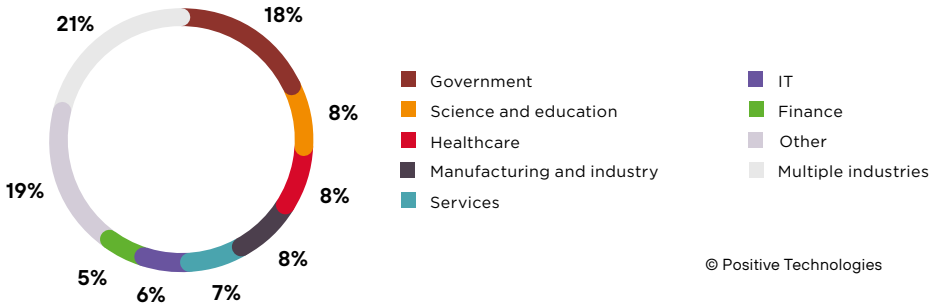

Figure 2. Categories of victim organizations

18% of attacks were aimed at individuals

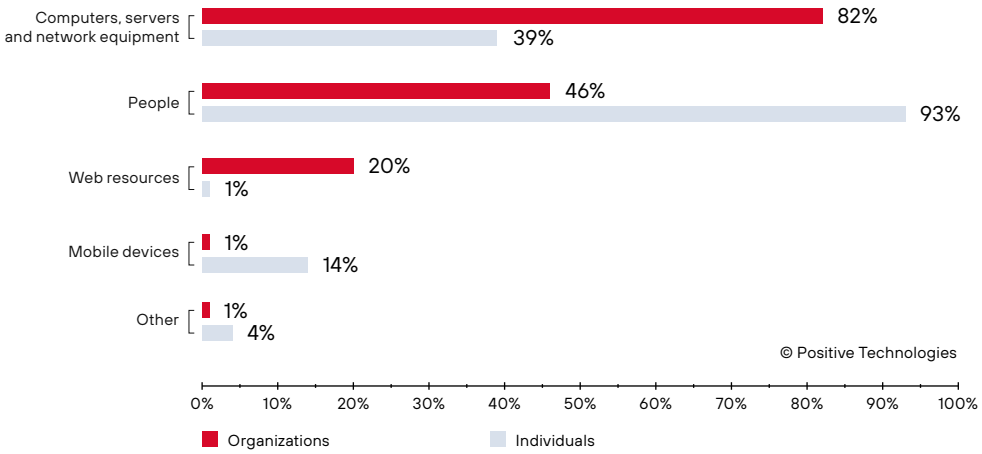

Figure 3. Attack targets (percentage of attacks)

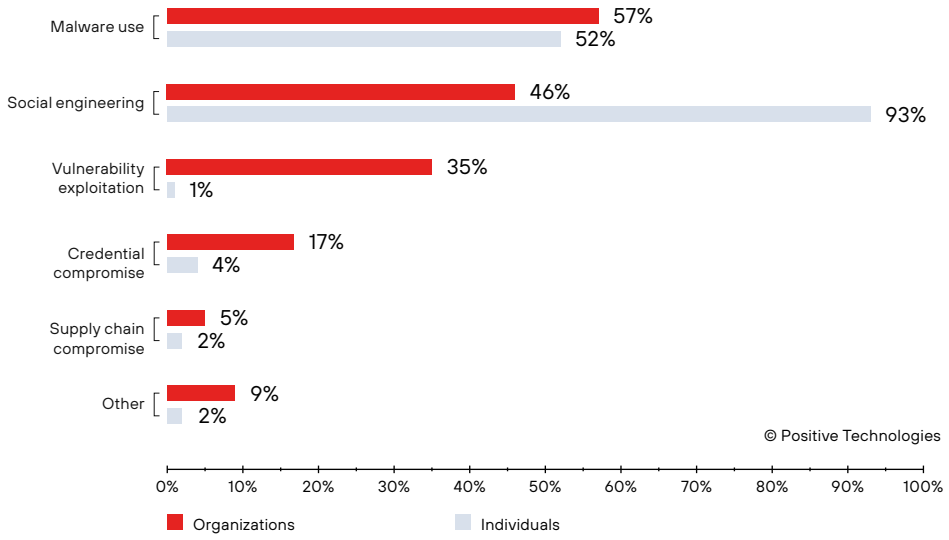

Figure 4. Attack methods (percentage of attacks)

67% of attacks were targeted

	Distribution of cyberattacks by target, method, consequence, and victim category	Victim categories: Government	Manufacturing and industry	Science and education	Services	IT	Healthcare	Finance	Other	Multiple industries	Individuals
	Total attacks	**115**	**51**	**52**	**44**	**38**	**52**	**30**	**122**	**132**	**138**
Target	Computers, servers, and network equipment	90	48	49	29	33	44	27	93	111	54
	Web resources	45	4	10	17	4	2	4	35	9	2
	People	48	23	30	15	16	28	16	43	76	129
	Mobile devices	1					1	1		3	20
	Other			1		1			2	3	5
Method	Malware use	64	35	44	12	22	25	19	55	89	72
	Social engineering	48	23	30	15	16	28	16	43	76	129
	Credential compromise	18	12	12	8	14	16	2	17	6	6
	Vulnerability exploitation	27	26	8	15	11	16	11	48	63	2
	Supply chain compromise	5	1	5	2	2	2	1	6	5	3
	Other	22	2	1	7	3		3	15	7	3
Consequences	Leak of confidential information	42	31	34	24	28	44	20	57	55	88
	Disruption of core activity	64	26	38	14	14	18	5	43	15	4
	Direct financial losses	3	2		3	3	2	2	15	13	28
	Damage to national interests	39	6						9		2
	Use of company or individual resources to carry out attacks	2	1	1	7	5	1	3	7	14	2
	Other		1				1			8	11
	Unknown	22	5	3	4	3	1	5	20	47	21

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

Attack consequences

More than half of attacks on organizations in Q3 2022 involved confidential information leaks: this type of consequence increased by 13 percentage points and reached 53% versus 40% in Q2 2022. Correspondingly, the share of attacks that disrupted core operations of organizations dropped from 50% to 37%. Cybercriminals seem to be partially shifting their focus to stealing confidential information.

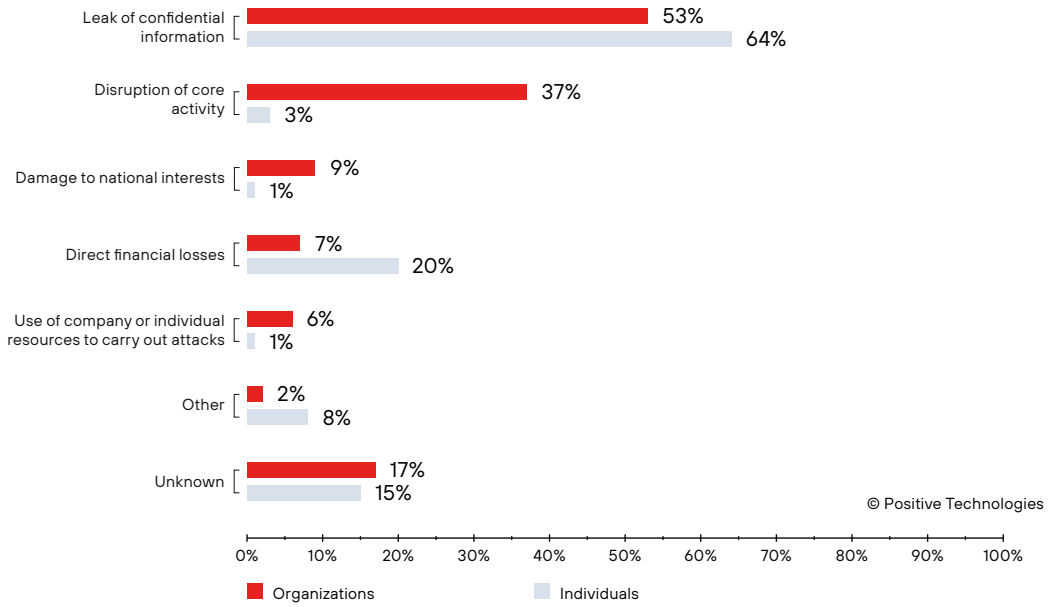

Figure 5. Attack consequences (percentage of attacks)

Hunting for credentials

Credentials increased from 9% to 17% of data stolen in attacks on organizations. This was made possible by intensified distribution of phishing kits, which led to numerous credential harvesting campaigns.

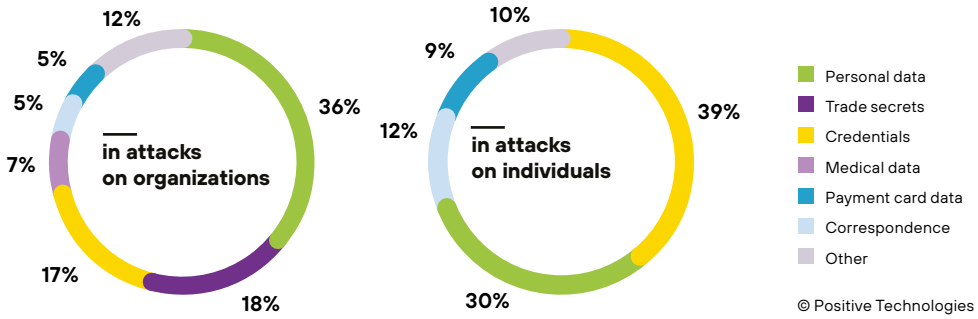

Figure 6. Types of data stolen

[1] The group announced that it was terminating its operations and shut down its servers and the website with victim data.

Attackers continue taking advantage of people's weaknesses and gullibility. The share of social engineering attacks remains persistently high: 93% of Q3 attacks involved the human factor. Security tools are constantly improving, making it more difficult for attackers to access the corporate infrastructure without being detected, so cybercriminals are forced to resort to social engineering. For example, a member of the notorious Conti group (their attacks caused a state of emergency in Costa Rica) mentioned once: "We can't win the technology war because on this ground we compete with billion-dollar companies, but we can win the human factor."

Stolen data made publicly available and offered for sale

As the market for cybercrime services is expanding, some companies find out they have been hacked only when cybercriminals start selling the stolen information at a high price on illicit forums. This was the case with the Singapore division of Starbucks, the popular coffeehouse chain: the attack was revealed in September when a cybercriminal offered to sell a database containing personal data of over 219,000 Starbucks customers on a hacking forum.

Major data leaks affected the citizens of Indonesia: a user of a hacking community forum offered to sell an archive with personal data of 105 million people, which is nearly 40% of the country's population. The data was likely stolen from the General Elections Commission of Indonesia. The data set included full names, dates of birth, and other sensitive information; it was offered for $5,000. An earlier case involved an archive with registration data of roughly 1.3 billion Indonesian SIM cards (with phone numbers and their owners' identity document information) offered for $50,000.

Q3 also witnessed a wave of attacks carried out by the Desorden group, previously known as chaoscc; these attacks stirred activity on cybercriminal forums. The group first used the new name in 2021 when attacking Asia-based organizations. Desorden mainly targets high-revenue companies and demands a ransom for non-disclosure of stolen sensitive information.

Malware: more attacks on Linux environments

In Q3, the share of malware attacks remained at the same level as in the previous quarter: malware was used in 57% of attacks on organizations and in 52% of attacks on individuals. Ransomware is still the most common malware type used against organizations, while individuals were more likely to suffer from spyware (46%).

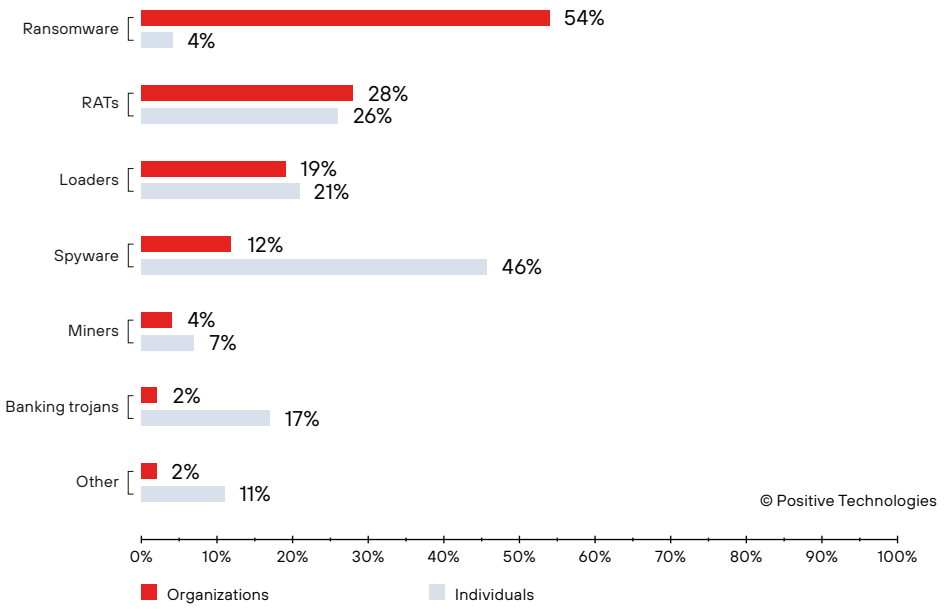

Figure 7. Types of malware (percentage of malware attacks)

Spyware

Since the second half of 2021, we've seen a continued rise in spyware attacks on individuals: attackers are increasingly focusing on stealing personal data and credentials from victims' personal devices. This can lead to compromise of corporate systems, because many employees work remotely and use their personal devices for work purposes. After a brief calm period, Raccoon Stealer (spyware popular among cybercriminals) is coming back with enhancements to its performance and ability to avoid detection.

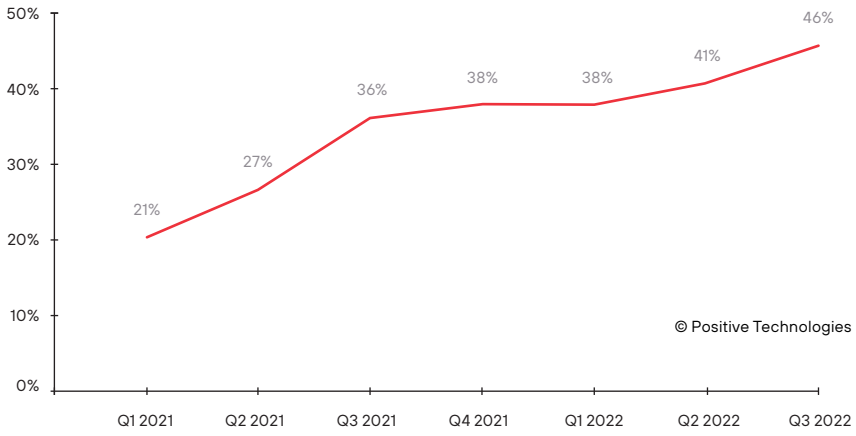

Figure 8. Spyware attacks (percentage of total malware attacks on individuals)

Compared to the previous quarter, there was little change in the methods of malware delivery in attacks on organizations: attackers relied heavily on phishing emails and penetrated corporate systems by compromising credentials and exploiting vulnerabilities.

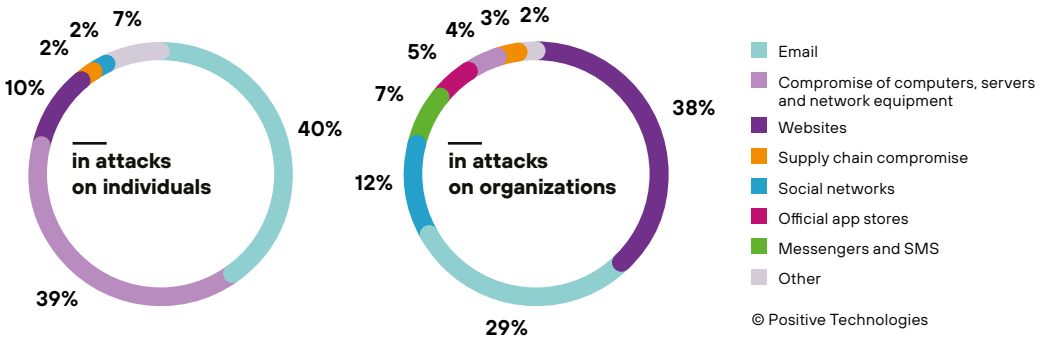

Figure 9. Malware distribution methods

In attacks on individuals, malware was mostly delivered by attackers via various websites (38%). Researchers found an interesting malware bundle specimen distributed as a self-extracting archive. Its main payload was the RedLine stealer, but the most ingenious part was its self-propagation functionality: one of the executable files downloaded a video and a text file with the video description containing malicious links, while another file uploaded that video to YouTube via the Chrome API.

Linux in danger

Many virtualization solutions and cloud technologies are based on Linux. The landscape of attacks against such solutions is expanding daily, and their consequences are worsening due to the growing popularity of virtualization and cloud technologies in business processes. Q3 saw a noticeable increase in the share of malware attacks affecting Linux: from 12% in Q2 to 30% in Q3.

Intezer researchers reported a new malware called Lightning. It is a modular malware framework with a wide range of capabilities: it can install rootkits and other payload types, and communicate with the command-and-control server in active and passive mode via a secure channel. Due to the growing adoption of Rust (a programming language that enables development of cross-platform software), a new attack framework called Manjusaka emerged. It was discovered in the wild by Cisco Talos researchers. This framework is particularly dangerous, because it can be used to attack both Windows and Linux, while its recent cross-platform implants and a new way of communicating with the command-and-control server allow attackers to successfully bypass defenses. Cross-platform frameworks, including Manjusaka, are an emerging threat with more destructive potential than the well-known Cobalt Strike. Availability of such tools on the black market—as was the case with Brute Ratel, which was cracked and shared across cybercriminal forums—can cause a significant increase in cyberattacks on the most common operating systems.

According to the IBM Security X-Force report, the number of new ransomware tools targeting Linux increased 2.5 times compared to 2021. Q3 2022 saw yet another case of ransomware being adapted to Linux: the infamous Hive group, which attacked the healthcare system of Costa Rica in Q2 2022, developed a new Hive ransomware version for Linux. The new version features an enhanced encryption algorithm, better evasion capabilities, and updated command-line parameters for running the payload.

Such sophisticated, well-designed malware tools for Linux have been appearing at an alarming rate, which requires users to be extra vigilant. Do not click on suspicious links and avoid opening unverified attachments. Do not download software from unofficial or unreliable sources: this can lead to your devices becoming compromised. Developers need to be cautious when downloading libraries, frameworks, and add-ons, and use only trustworthy remote repositories.

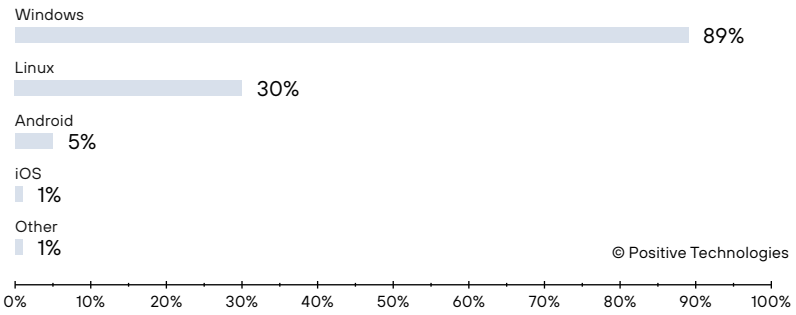

Figure 10. Target OS in malware attacks (percentage of attacks)

New botnets

New players are entering the scene: this summer, Cloudflare researchers reported the emergence of a powerful botnet, which was used in a major DDoS attack. At its peak, the botnet generated 26 million requests per second using only 5,067 bots. For the sake of comparison: experts estimate that last year the Mēris botnet commanded more than 200,000 infected devices, with a peak capacity of 21.8 million requests per second. Cloudflare researchers named the new botnet Mantis and observed it attacking nearly 1,000 Cloudflare customers over the course of several weeks. Unlike previously known botnets that use IoT devices, Mantis infects and exploits virtual machines and powerful servers, thus leveraging more computing power and increasing the overall attack strength.

Ransomware threat to the education sector

In Q3, ransomware activity was as high as in the previous quarter; this is due to the emergence of several new players (RedAlert, Luna, 0mega), new black-market offers of access to corporate networks, and the return of social engineering campaigns. More than half of all attacks on organizations (54%) involved ransomware.

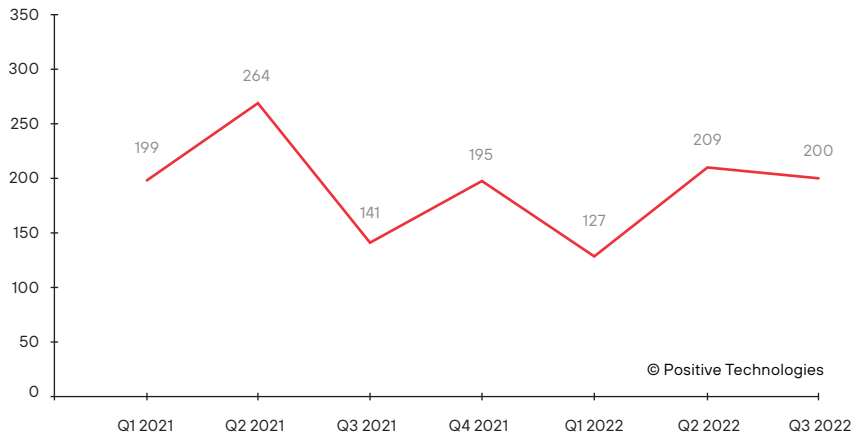

Figure 11. Number of ransomware attacks

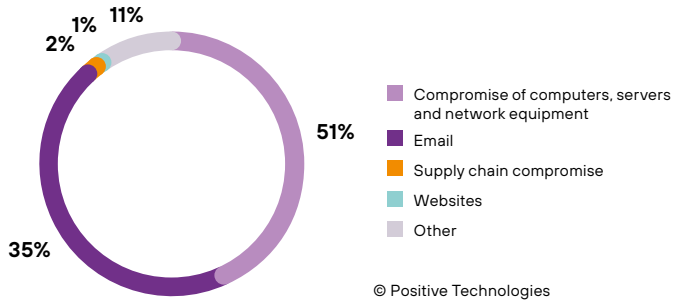

Figure 12. Ransomware distribution methods in attacks on organizations (percentage of malware attacks)

The share of ransomware delivered via email continues to decline (down 14 percentage points from the previous quarter), while computer and network device compromise increased by 3 percentage points from the previous quarter (reaching 51%), which can be attributed in part to access brokers who offer their services to penetrate compromised systems. On the Exploit forum, for example, a cybercriminal claimed to have access to the infrastructure of an IT service provider and was looking for partners to help the criminal exploit it. More information about the cybercriminal market trends, sale of access to corporate networks, and pricing of these services is provided in another study by Positive Technologies.

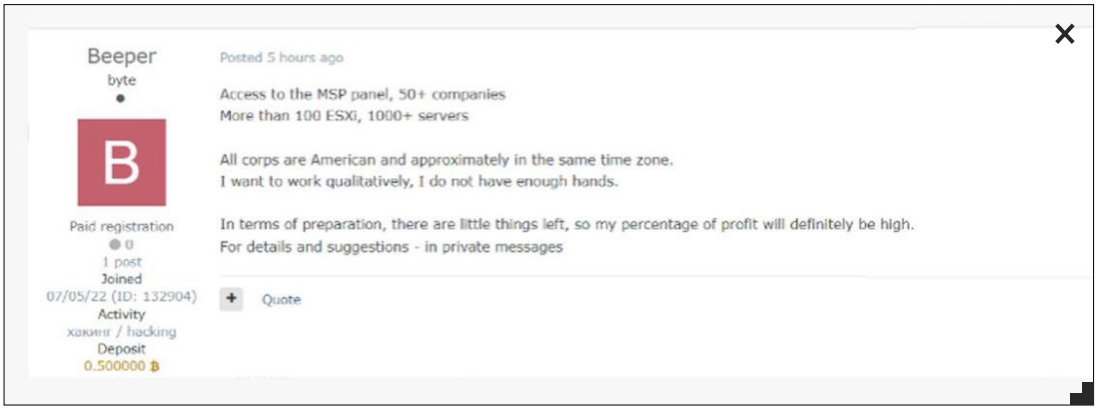

Figure 13. Advertisement offering access to corporate infrastructure

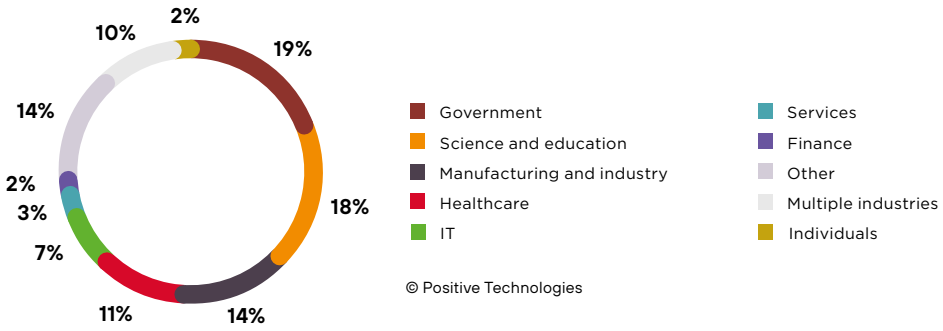

Figure 14. Ransomware attacks by industry sector

In Q3, ransomware groups shifted their focus to the education sector, which accounted for 18% of all attacks (up 7 percentage points compared to the previous quarter). The Vice Society ransomware group managed to carry out a major attack on the Spanish National Research Council (CSIC), resulting in a disconnection of more than 100 CSIC centers and a personal data leak. Educational institutions were not spared from ransomware attacks: due to such an attack, the Waterloo Region District School Board had to restore most of its systems and notify students, staff, and graduates who were affected by the personal data leak.

Attacks on the energy sector

Industry accounted for 14% of the total number of ransomware attacks. In Q3, ransomware groups targeted the energy sector, in particular:

- In July, client portals of Creos Luxembourg, a gas pipeline and electricity network operator, were unavailable due to an attack by the BlackCat ransomware gang. The attackers stole technical documents, along with information about the operator's contracts and customers.
- Attacks on the systems of the Italian oil-refining giant Eni and energy agency Gestore dei Servizi Energetici were carried out only a few days apart. Both attacks led to large-scale leaks of confidential information, unavailability of some systems, and disruption of customer service.
- The Ragnar Locker group attacked the Greek gas pipeline operator DESFA, disrupted some of its systems, and stole more than 350 GB of sensitive data.

Attacks on critical infrastructure facilities, including energy companies, and the resulting disruption of their operations can lead to serious consequences: many still remember the attack on Colonial Pipeline, which disrupted fuel supply and caused fluctuations in fuel prices, and the attack on the Venezuelan hydroelectric power plant that led to power outages throughout the country.

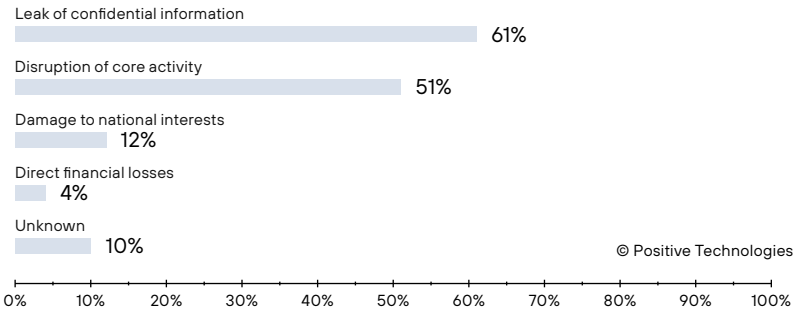

Figure 15. Consequences of attacks on industry sectors (percentage of attacks)

Social engineering on the rise

We saw an increase in the number of mass social engineering attacks in Q2 2022, and Q3 continued this trend: attackers are leveraging the human factor to overcome technical cybersecurity mechanisms.

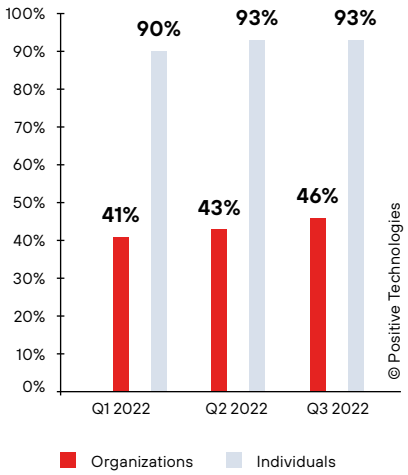

Figure 16. Percentage of social engineering attacks

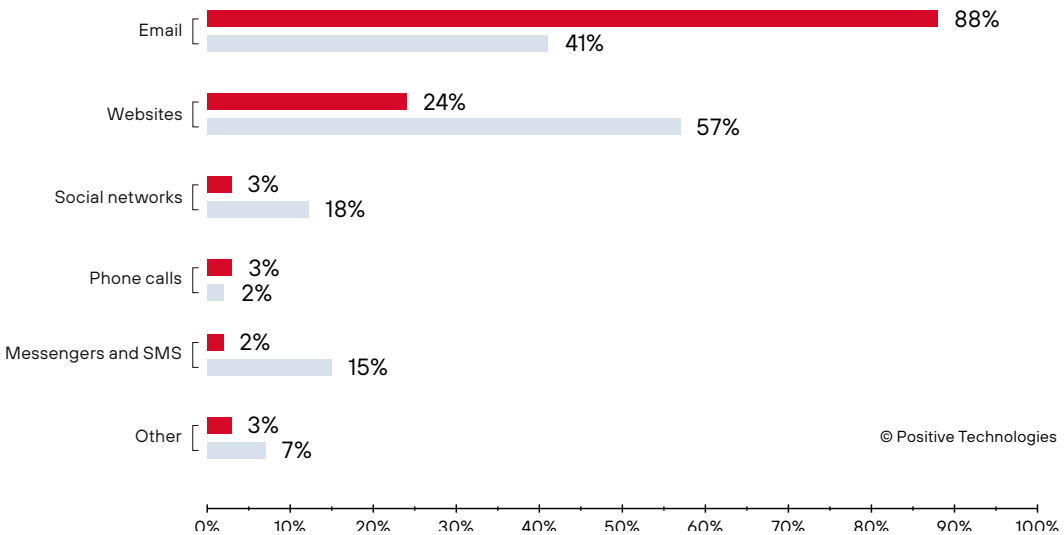

Figure 17. Social engineering channels used by attackers

To deceive both users and antivirus software, cybercriminals usually combine multiple tactics.

Learning from ransomware operators

To make social engineering methods more effective, attackers don't have to invent something fundamentally new: they can learn from their comrades in crime—for example, ransomware operators. In one of the phishing attacks in the middle of summer, attackers used a countdown timer. First, victims received an email about a suspicious login attempt. To verify the email account, the victims were urged to follow a link and then required to enter their account credentials within an hour to prevent the account from being deleted. In addition to the countdown timer, the page displayed a randomly generated list of accounts (assigned to the domain belonging to the target organization) that the phishers claimed to be deleting at that moment.

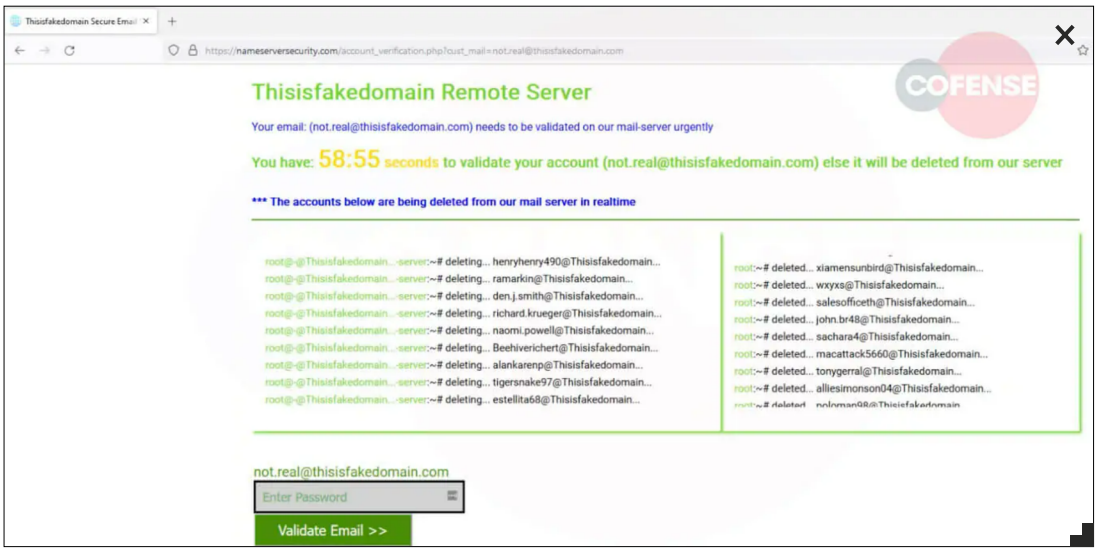

Figure 18. Phishing website

Ransomware operators also use social engineering in their attacks: this summer saw a resurgence of BazaCall attacks that we covered in our Q3 2021 report. The BazaCall (or BazarCall) technique was initially used by the Ryuk ransomware group. The attack started with an email informing the victim about a subscription payment that is due soon. The email also included a phone number for canceling the payment. Victims calling that number reached a fake call center operator who convinced the caller to either download a specific file or start a remote access session to resolve the issue. As a result, the intruder compromised the network and could start deploying the ransomware.

Telegram bots for data exfiltration

Previously, cybercriminals mostly sent stolen information to disposable email accounts, but now they also use Telegram. Due to the encrypted nature of messaging in the app, the data is kept secret, and the traffic doesn't appear suspicious to organizations where the messenger is used.

In early 2022, we wrote about Raccoon stealer operators using Telegram as a control and command tool. In the recent phishing campaigns, attackers resorted to the same method of sending stolen data. One of these attacks targeted DHL customers: in July, Sucuri researchers discovered a fake shipment tracking page that imitated the original DHL page, but harvested personal and payment data and sent them as HTTP requests to the API URL of the attacker's Telegram bot.

Short-lived and legitimate domains

Before the victim can read a malicious email, it first has to avoid anti-spam filters and find its way into the inbox. Scammers employ various techniques to bypass detection by security tools. For example, they can use malicious webpages hosted on legitimate domains, making the emailed links to phishing websites seem harmless. In August, for example, Avanan reported a spike in attacks in which cybercriminals used phishing websites hosted on Amazon Web Services (AWS), a popular cloud storage and hosting solution. The researchers call this attack technique The Static Expressway: email services that use static allowlists or blocklists are not immune to these attacks, because they consider legitimate AWS domains as safe resources.

An interesting technique was employed in a phishing campaign aimed at stealing account credentials of Coinbase crypto exchange users: the phishing domains remained active for extremely short periods of time, with most pages being available for less than two hours on average. In most cases, such phishing pages avoid being archived, because they are taken offline before search engines index them. In addition, cybercriminals restrict access to their phishing websites by geolocation or IP address range, allowing only the intended victims to connect. This complicates the work of security researchers: even if a phishing page is detected while it is still live, a researcher would need to spoof the restrictions to be able to access the website.

In another attack targeting customers of Indian banks, attackers took advantage of the hosting solution's capability to create preview domains, which allows you to view the website content before it becomes publicly available. Such phishing websites could exist for up to five days.

Phishing-as-a-service

At the beginning of the year, we predicted that phishing-as-a-service would spread, and now we indeed see it gaining momentum. In Q3 2022, the number of large-scale social engineering campaigns against organizations increased by 41% and by 34% against individuals compared to Q2. This growth is primarily caused by widespread use of phishing kits. A phishing kit is a ready-to-use collection of software tools for phishing attacks. It can also include preconfigured phishing pages, data entry forms, scripts for sending messages to victims, and scripts for sending stolen data to attackers.

How phishing-as-a-service works

Phishing kits are easy to use, enabling even low-skilled attackers to carry out phishing attacks. Some phishing kits sell for as little as $7 (and some repositories are available free of charge), while harvested credentials may cost many times as much.

Cybercriminal platforms are flourishing, offering more opportunities to buy and sell cybercriminal services, including phishing. This summer, IronNet researchers came across a large-scale campaign that involved the new Robin Banks platform selling phishing kits to defraud customers of well-known banks and online services. Platform users can buy a preconfigured toolset or create their own custom-made phishing kit. Access to a single page with any future updates and 24/7 support from the platform costs $50 per month.

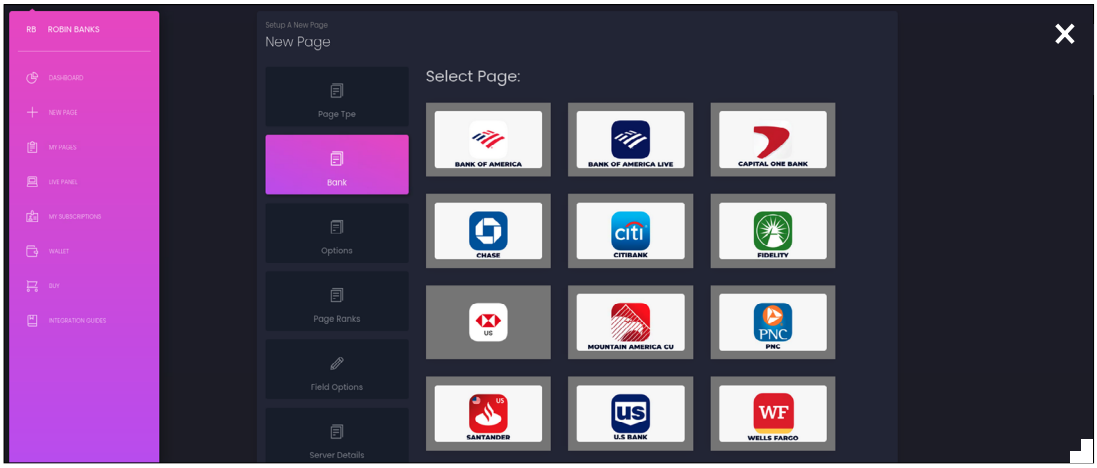

Figure 19. Robin Banks platform interface

Phishing kit updates

[2] Open Redirect is a vulnerability that allows attackers to modify URL parameters and redirect users to untrusted resources such as phishing websites..

Phishing kits are being increasingly employed in phishing campaigns, and their features are being constantly updated. In early August, for example, Resecurity researchers detected a surge in attacks using LogoKit. This phishing kit leverages Open Redirect[2] vulnerabilities in popular online services and apps. One of the campaigns using this phishing kit was detected in July; it targeted Office 365 users from the U.S. and Latin America. Initially, the victim received an email notifying them that their password was about to expire. To keep the current password, the user was urged to click the link in the email. The embedded link led to a fake credential entry form where the email address field was populated automatically, creating the illusion that the user had visited the website before. To add to the air of legitimacy, when a user follows the link, LogoKit retrieves the company logo from open sources and automatically embeds it into the fake entry form.

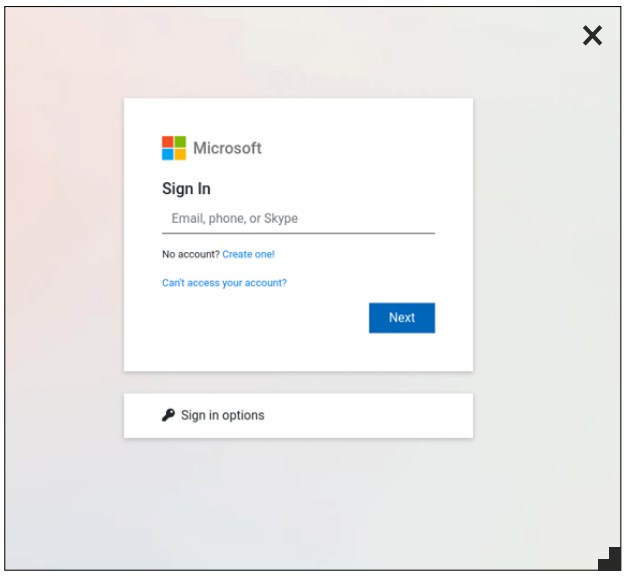

Figure 20. Fake entry form

Quantity transforming into quality

Another phishing kit targets PayPal users. To deliver it, attackers hacked legitimate websites with weak passwords and injected malicious code. Such an attack has huge potential, because over 400 million individuals and companies use PayPal as an online payment solution.

This campaign is also impressive in terms of the size and scope of stolen data: attackers were able to compromise both credentials and ID documents (passports and driving licenses), which is unusual for phishing kits. The data theft scheme started with a CAPTCHA challenge, a step that created a false sense of a secure website. After that, the victims were asked to log into their PayPal account by entering their email address and password in a fake entry form. Then, under the pretense of "unusual activity" associated with the account, the attackers requested additional verification information: personal and payment data, residential address, and even the victim's mother's maiden name. The scam didn't stop at that: users were urged to link their PayPal account to their email account and upload personal identification documents (for example, a passport or driving license).

To avoid becoming a victim of cybercriminals, we recommend shopping only in trustworthy online stores and paying close attention to URLs in the browser address bar. If you get a notification about suspicious activity associated with your account, don't click the link in the notification; instead, check the information on the provider's legitimate website.

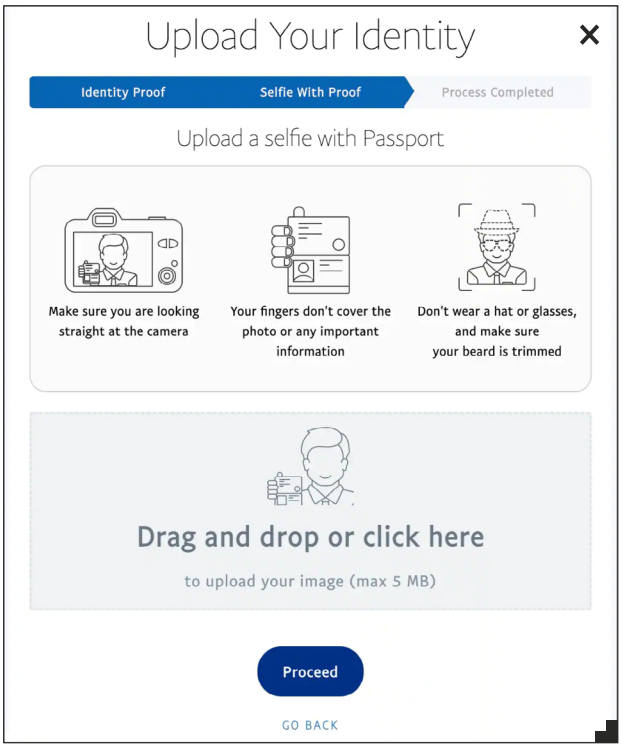

Figure 21. Fake data upload form

Bypassing multifactor authentication

Multiple identification factors may not be enough anymore: researchers have detected large-scale phishing campaigns that can bypass multifactor authentication. Starting in June 2022, Zscaler's ThreatLabz researchers noticed a spike in attacks using phishing kits that employ reverse proxy servers. The operation is still ongoing, and new phishing domains are registered nearly every day.

This technique with reverse proxy servers is called adversary-in-the-middle (or man-in-the-middle): the attacker secretly operates between the victim and the server of the email provider. When the user navigates to a phishing page, the reverse proxy server displays the legitimate login form. After the victim enters their credentials and the one-time password (OTP), the phishing kit forwards that information to the actual platform server and intercepts the resulting session cookie. The attacker can use this stolen authentication cookie to log into the compromised user's account, bypassing multifactor authentication.

With multi-factor authentication becoming a common part of corporate security policies, cybercriminals are increasingly turning to reverse proxy servers. Responding to high demand for reverse proxies, a phishing-as-a-service platform called EvilProxy has emerged, promising to bypass multifactor authentication on Apple, Google, Facebook, Microsoft, Twitter, GitHub, GoDaddy, and even PyPI. Such services enable low-skill cybercriminals who don't know how to set up reverse proxies to steal poorly protected accounts. EvilProxy also offers detailed tutorials and a rich collection of phishing pages imitating popular internet services.

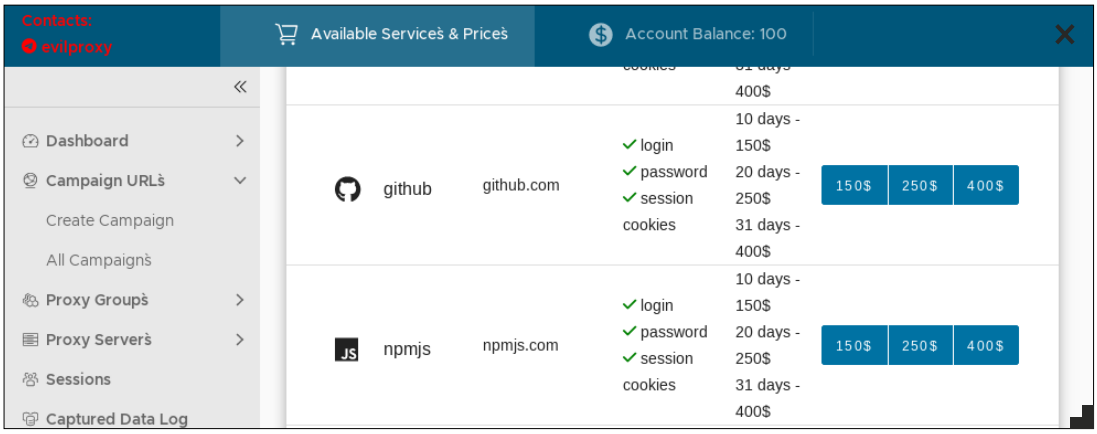

Figure 22. Phishing campaign options

Mass attacks on web applications

Vulnerable websites always attract cybercriminals: the number of attacks that involve exploitation of web vulnerabilities has increased by 67%. By exploiting flaws in web applications, attackers can gain access to internal networks of organizations and continue the attack by stealing an online store customer database or launching a mass attack on website visitors. In Q3, mass attacks on web resources affected an increasing number of victims: as new vulnerabilities were discovered in popular CMSs, attackers mainly targeted customers of compromised websites.

Popular vulnerabilities

New vulnerabilities, not to mention exploits for them, always cause excitement among cybercriminals, especially if they affect widely used CMSs.

In September, Wordfence Threat Intelligence researchers warned about mass attacks on websites that use the WPGateway premium plugin. The CVE-2022-3180 vulnerability allows unauthenticated attackers to add a malicious administrator, gaining control over the breached web resource. Over the course of 30 days, the researchers registered over 4.6 million attacks attempting to exploit the new vulnerability on more than 280,000 websites.

However, it is not uncommon for previously discovered vulnerabilities to suddenly regain popularity. Sometimes it can be explained by exploits for these vulnerabilities being openly distributed on illicit forums: this way, more cybercriminals can use them. In July, for instance, researchers discovered a sudden spike in attacks targeting websites that use the vulnerable Kaswara Modern WPBakery Page Builder plugin. This previously disclosed vulnerability is known as CVE-2021-24284. It allows unauthorized attackers to upload arbitrary files (for example, malicious web shells), leading to code execution and complete website takeover. As the plugin was closed without a patch, all its versions are affected by this vulnerability. Starting from July 4, attackers scanned an average of 443,868 websites per day, trying to find the plugin and exploit the vulnerability.

In Q3 2022, Sansec analysts also registered a surge in attacks aimed at exploiting a critical vulnerability in the Magento platform (CVE-2022-24086). Improper input validation during the checkout process allows attackers to execute arbitrary code. Researchers discovered three variations of attacks that exploited this vulnerability to inject a remote access trojan.

To reduce the risk of web resource compromise, keep your software up-to-date, including CMS and all plugins. We recommend adhering to your vendor's official guidelines on how to secure your website amid widespread exploitation of new vulnerabilities. Be sure to use web application firewalls (WAFs) that protect web application from attacks, in particular from exploitation of vulnerabilities for which no patches are available yet.

Threats to e-commerce

Positive Technologies Expert Security Center (PT ESC) discovered over 12,000 compromised websites running on Bitrix: their pages were injected with a link to a malicious JavaScript. If a user navigated to a compromised website, the script checked whether that visit was directed by a search engine and whether the user visited other compromised pages on that day. If both conditions were met, the script redirected the user to a phishing page masquerading as a legitimate resource—for example, a well-known online store. In the end, the cybercriminals obtained the victim's payment card data.

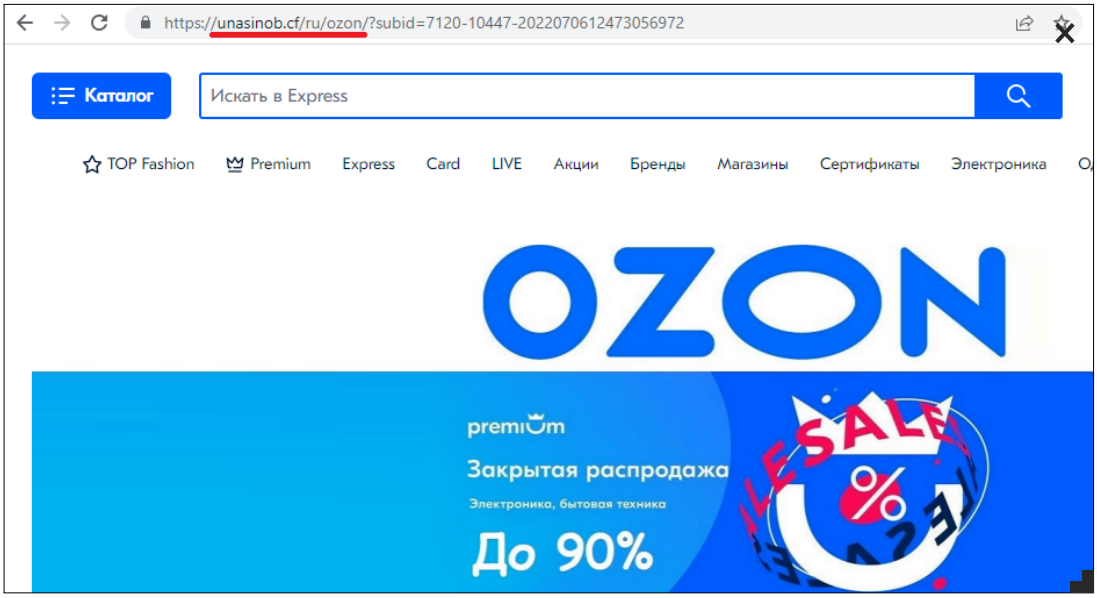

Figure 23. Phishing page

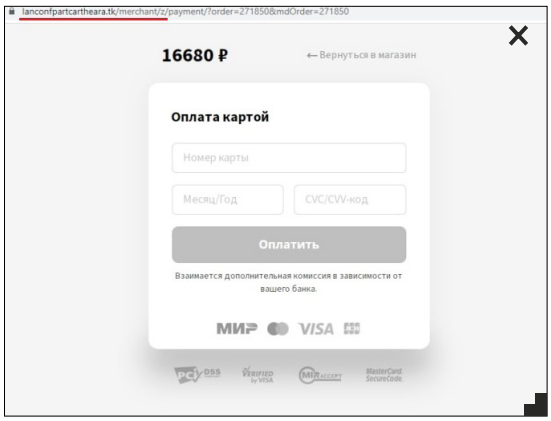

Figure 24. Phishing payment form

In another series of attacks, cybercriminals exploited Magento vulnerabilities, accessing the website's source code to inject a web skimmer. A web skimmer is a script designed to steal data from checkout pages and payment forms. Notably, the script was obfuscated and also checked whether developer tools were open in the browser. To make the process appear legitimate, the script even checked the format of data entered by victims—for example, the length of the card number.

To inject skimmers, some cybercriminals use legitimate tools that can be added to the page code. For example, Google Tag Manager (GTM) containers are frequently used for internet marketing, as well as tracking and analyzing customer behavior on websites. In 2021, Recorded Future researchers found malicious scripts hidden within GTM containers that functioned either as skimmers or as downloaders for installing skimmers. In July 2022, the researchers discovered new, obfuscated variants of this malicious code. The GTM-based web skimmers continued to infect new domains in August 2022. In September, over 165,000 payment card records belonging to visitors of infected e-commerce websites were posted on dark web forums. By using legitimate tools such as GTM containers, cybercriminals can update malicious scripts without accessing the breached websites directly, thus avoiding detection.

In addition, cybercriminals infected a large number of vulnerable websites with phishing tools designed to steal users' data. We described one of these attacks in the section on the phishing-as-a-service model: cybercriminals hacked WordPress-based websites with weak passwords and installed a file management plugin that was subsequently used to upload a phishing kit that targeted PayPal users. Such proliferation of web skimmers and phishing tools could be a sign that cybercriminals are preparing for Black Friday and other seasonal sales: the more websites are infected, the more user data will be harvested.

When shopping online, use only well-known, reliable online stores and double-check URLs in the browser address bar. Before entering your payment and personal details, make sure that the page is genuine, and a secure connection is used. Do not click on suspicious links and avoid opening email attachments if you are not sure that they come from a trusted sender. To shop online, we recommend using a separate payment card (a virtual card will do), keeping only small amounts of money on it, and setting limits on online purchases.

About the report

This report contains information on current global information security threats based on Positive Technologies' own expertise, investigations, 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.