# Acronis Cyberthreats Report, H1 2024:

Email attacks surge 293%, new ransomware groups emerge.

Acronis Threat Research Unit

## Executive summary

The biannual Acronis Cyberthreats Report covers the global threat landscape as encountered by Acronis sensors and analysts in the first half of 2024. General malware data presented in the report was gathered from January to May of 2024 and reflects threats targeting endpoints we observed in this time frame.

Based on over 1,000,000 unique endpoints distributed around the world, the report includes statistics focused on threats targeting Windows operating systems, as these are much more prevalent than those targeting macOS and Linux.

### Key findings:

- Bahrain, Egypt and South Korea were the most targeted countries for malware attacks in Q1 2024.
- Nearly 28 million URLs were blocked at the endpoint by Acronis in Q1 2024, a 3% increase over Q4 2023.
- 27.6% of all received emails were spam, and 1.5% contained malware or phishing links.
- Each malware sample lives an average of 2.3 days in the wild before it disappears — 82% of samples were only seen once.
- There were 1,048 publicly reported ransomware cases in Q1 2024, a 23% increase over Q1 2023.
- Three highly active groups were the primary contributors to ransomware attacks, collectively responsible for about 35% of the attacks.
- LockBit accounted for 20% of ransomware attacks, followed by BlackBasta and Play, with 7.1% and 7.0% respectively.

### Top cybersecurity trends in the first half of 2024:

- Ransomware continues to be a major threat to small and medium-sized businesses, including government, health care and other critical organizations. Recently, ransomware makers have abused vulnerable drivers to get a foothold in systems and disable security tools.
- More IT companies are being compromised, threatening the overall cybersecurity industry.
- AI is a commonly used tool in cyberattacks, but it has not assumed the full cyberattack kill chain.
- In the first quarter of 2024, Powershell T1059.001 was the most frequently detected MITRE technique.
- The number of email attacks detected in H1 2024 surged by 293% compared to the first half of 2023.

# Key cyberthreats and trends in H1 2024

### Ransomware gangs continue to wreak havoc

The following ransomware gangs were the most active in H1 2024 in terms of total numbers of victims:

- LockBit (413)
- Play (135)
- 8Base (115)
- BlackBasta (113)
- Hunters International (100)

February 2024 marked a significant milestone in the battle against cybercrime: the dismantling of the infamous LockBit ransomware gang (at least partially). This criminal organization had been a thorn in the side of businesses and governments worldwide, perpetrating some of the most disruptive and costly cyberattacks in recent history.

Operation Cronos, led by the U.K.'s National Crime Agency (NCA), with support from Europol, Eurojust and global law enforcement agencies, disrupted LockBit ransomware gang operations. The task force seized control of 34 servers that comprised LockBit's primary infrastructure, as well as 14,000 accounts used for hosting tools and storing stolen data. Additionally, authorities confiscated 200 cryptocurrency wallets and 1,000 decryption keys, which were instrumental in developing a publicly available decryptor tool.

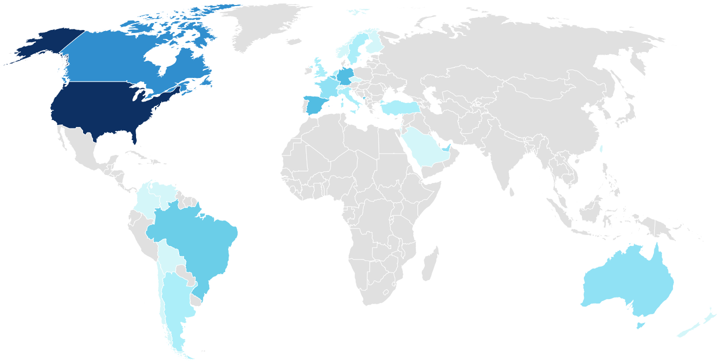
Another big player, the BlackCat ransomware group, also known as ALPHV, vanished in March after what appears to be an exit scam following a substantial $22 million payout. The initial signs of the exit scam emerged when BlackCat's darknet website displayed a banner claiming it had been seized by law enforcement. This was quickly debunked by cybersecurity experts who noted inconsistencies in the source code of the seizure notice, indicating it was a fraudulent claim designed to mislead affiliates and victims. The NCA confirmed they had no involvement in any operation against BlackCat at the time.

### MSPs under attack

MSPs were under constant attack from January to May 2024. Our analysis revealed that attackers predominantly used email phishing campaigns, followed by exploiting vulnerabilities in RDP and remote access tools.

| Attack vector | Number of attacks |
|---|---|
| Phishing | 27 |
| RDP | 22 |
| Unpatched vulnerabilities | 21 |
| Abuse of valid accounts / credentials | 13 |
| Trusted relationship | 7 |

**Most targeted countries for attacks on MSPs**



### Phishing and malicious emails remain the main vector of infection

The following email and phishing statistics are aggregated from Acronis Cyber Protect Cloud with Advanced Email Security, which is powered by Perception Point. The data was gathered in the first half of 2024 and is combined with Acronis telemetry data for malware and URL blocks on the endpoints.

In the first half of 2024, organizations experienced a significant surge in email communications, with the number of emails per organization increasing by 25%. This rise in email volume has been paralleled by a concerning 47% increase in email attacks targeting these organizations. Alarmingly, 40% of users faced at least one attack. Finally, social engineering increased 5% since H1 2023, while malware attacks decreased from 11% in H1 2023 to 4% in H1 2024.

Currently, one in three emails is unsolicited. The spam rate has dropped to 27.6%, an improvement from 30.3% in the first half of 2023. Despite this reduction, the proportion of emails with malicious content has increased slightly to 1.5%, up from 1.3% in the same period last year. This underscores the persistent issue of email threats, even as spam control has improved.

### Phishing trends

An emerging cybersecurity trend is login impersonation. In this scheme, an attacker sends an email to a user with a file attached. The attacker's display name is set to "Shared File Access," making the email appear to be a fax-to-email communication. The attached PDF contains a QR code that the user is instructed to scan to access the document. However, scanning the QR code directs the user to a fake Microsoft login page designed to steal their credentials.

### Soccer scam

A new scam has emerged in which individuals receive an email allegedly from UEFA EURO claiming the user has been randomly selected as a soccer fan to win a UEFA EURO 2024 getaway. The email includes a list of winners, with the recipient's name cleverly added as the last winner on the list. The email urges the recipient to click a "Next" button to confirm their response. Clicking the button redirects the user to a landing page with trivia questions about EURO 2024, which, regardless of the user's answers, leads to a congratulatory message stating they can purchase a MacBook Pro for only €2.00. The user is then taken to a form requesting personal information, followed by a fraudulent payment page asking for credit card details. Submitting this information sends it directly to the attackers. Additionally, a preselected checkbox at the bottom of the page consents to terms that could result in contractual complications and significant financial losses.

Another growing trend is attacks within collaboration tools, where phishing and advanced attacks comprise nearly 20% of the attacks and 82% comprise malware-based attacks.

### General malware threats

In January, about 17.9% of Acronis clients had at least one malware attack successfully blocked on their endpoints. The percentage peaked at 28% in April, dropping to 23.8% in June. These still high percentages suggest that, despite security awareness training and patching, about two out of every 10 threats makes it to the endpoint. Furthermore, because these statistics are based on endpoint detections, any proxy or email protection applied earlier in the chain did not prevent these threats.

Another prevalent trend in the first half of 2024 is malvertising, which continues to deceive users into downloading fake software by leveraging Google Ads and SEO poisoning.

Acronis has identified a 5% increase in the number of new malware samples appearing in the wild since Q4 2023. Independent malware testing lab AV-TEST recorded 328,960 new malware samples per day in Q1 2024, compared to 312,874 in Q4 2023. This proportion matches the number of new samples seen by Acronis Cyber Protection Operation Centers.

The average lifetime of a malware sample in June 2024 was a mere 2.3 days, after which it disappeared and was never seen again by Acronis. In May 2024, this figure was down to 2.1 days. Malware is shorter lived than ever, as attackers use automation to create new and personalized malware at blazing speeds in an effort to bypass traditional signature-based detection. Of all the samples observed, 82% were seen only once across our customer base.

## Normalized malware detections by focus countries

| Country | January 2024 | February 2024 | March 2024 | April 2024 | May 2024 |
|---|---:|---:|---:|---:|---:|
| Australia | 17.1% | 16.4% | 20.4% | 23.4% | 20.1% |
| Brazil | 22.6% | 23.3% | 31.1% | 31.7% | 28% |
| Canada | 8.2% | 9.2% | 11.2% | 14.4% | 12.1% |
| France | 14.4% | 19.4% | 24% | 26.7% | 20.4% |
| Germany | 20.2% | 21.7% | 25.6% | 27.5% | 23.7% |
| Italy | 18.2% | 13.2% | 27.9% | 30.1% | 26.8% |
| Japan | 14% | 20.9% | 15.7% | 16.7% | 14.1% |
| Netherlands | 18.4% | 20.4% | 25.9% | 26.1% | 21.9% |
| Singapore | 43.9% | 38% | 29.6% | 41.7% | 29% |
| South Africa | 14.2% | 33% | 25.9% | 27.9% | 23% |
| Spain | 32.2% | 16.6% | 40.5% | 37.5% | 31.2% |
| Switzerland | 17.3% | 22.5% | 24% | 24.8% | 20.4% |
| United Arab Emirates | 17.6% | 18.8% | 29.1% | 29.3% | 29.3% |
| United Kingdom | 13.8% | 17.5% | 20% | 19.5% | 16.5% |
| United States | 16% | 24.9% | 30.9% | 33.7% | 26.8% |

## Normalized ransomware detections by focus countries

| Country | Ransomware detections in Q1 2024 | Ransomware detections in April 2024 | Ransomware detections in May 2024 |
|---|---:|---:|---:|
| Australia | 2.6% | 1.1% | 0.7% |
| Canada | 5.5% | 2% | 1.7% |
| France | 4.1% | 1.6% | 1.3% |
| Germany | 13.4% | 5.4% | 4.5% |
| Italy | 1.9% | 0.8% | 0.5% |
| Japan | 16.5% | 5.6% | 4.5% |
| Netherlands | 4.3% | 1.8% | 1.5% |
| Spain | 4.5% | 1.1% | 0.9% |
| United Kingdom | 2.5% | 0.9% | 0.6% |
| United States | 5.4% | 1.7% | 1.7% |

## Top 15 countries: Blocked URLs, normalized

| Rank | Country | Percentage of blocked URLs in April 2024 |
|---|---|---:|
| 1 | India | 28.7% |
| 2 | Colombia | 27.3% |
| 3 | South Korea | 24.1% |
| 4 | Brazil | 21.8% |
| 5 | France | 21.5% |
| 6 | Mexico | 20.9% |
| 7 | United States | 19.6% |
| 8 | Japan | 17.7% |
| 9 | Netherlands | 16.7% |
| 10 | Singapore | 16.3% |
| 11 | Germany | 16.3% |
| 12 | Australia | 14.5% |
| 13 | Italy | 14% |
| 14 | United Kingdom | 10.8% |
| 15 | Canada | 6% |

Acronis

Learn more at
www.acronis.com