Acronis
TRU Security Day
Italy 2025

Cyber-stats you can use: Regional insights

Sergey Belov

Director of Information Security
TRU Team
Acronis

Acronis
Threat Research Unit

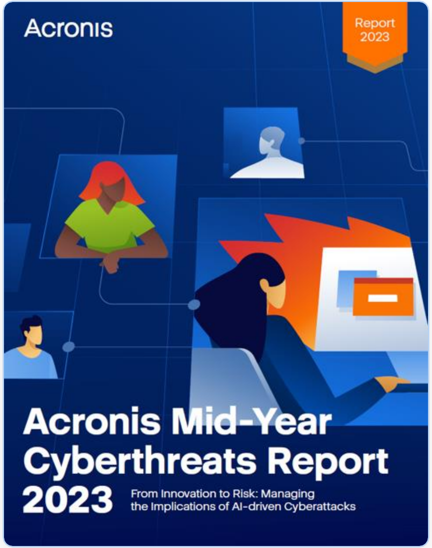
Acronis
Threat Research Unit

Intelligence-driven cyberthreat research and reporting

- Original threat research
- Community engagement
- Best practices recommendations
- Cyberthreat reports and analysis
- Collaborative events
- Partner briefings and support

Twice-per-year Cyberthreats reports

Started 2021



Acronis

Report 2023

Acronis Mid-Year Cyberthreats Report 2023

From Innovation to Risk: Managing the Implications of AI-driven Cyberattacks

Acronis

Report H2 2023

Acronis Cyberthreats Report, H2 2023:

Alarming rise in cyberattacks, SMBs and MSPs in the crosshairs

Acronis

Report H1 2024

Acronis Cyberthreats Report, H1 2024:

Email attacks surge 293%, new ransomware groups emerge

Acronis Threat Research Unit

Acronis

Report H2 2024

Acronis Cyberthreats Report, H2 2024: The rise of AI-driven threats

Acronis Threat Research Unit

H2 2024 Cyberthreats report

Key vectors of attacks on MSPs

- Phishing (34%)
- Unpatched vulnerabilities (19%)
- Remote Desktop access exploitation (15%)

More and more ransomware cases

- 1712 ransomware cases were publicly mentioned in Q4 2024
- Top contributors: RansomHub, Akira, Play and KillSec - 580 total victims

One critical vulnerability ruins everything

- Clop gang exploited vulnerability CVE-2024-55956 in Cleo file transfer software
- Last December Clop extorted 68 companies with this exploit
- The number of victims likely much higher

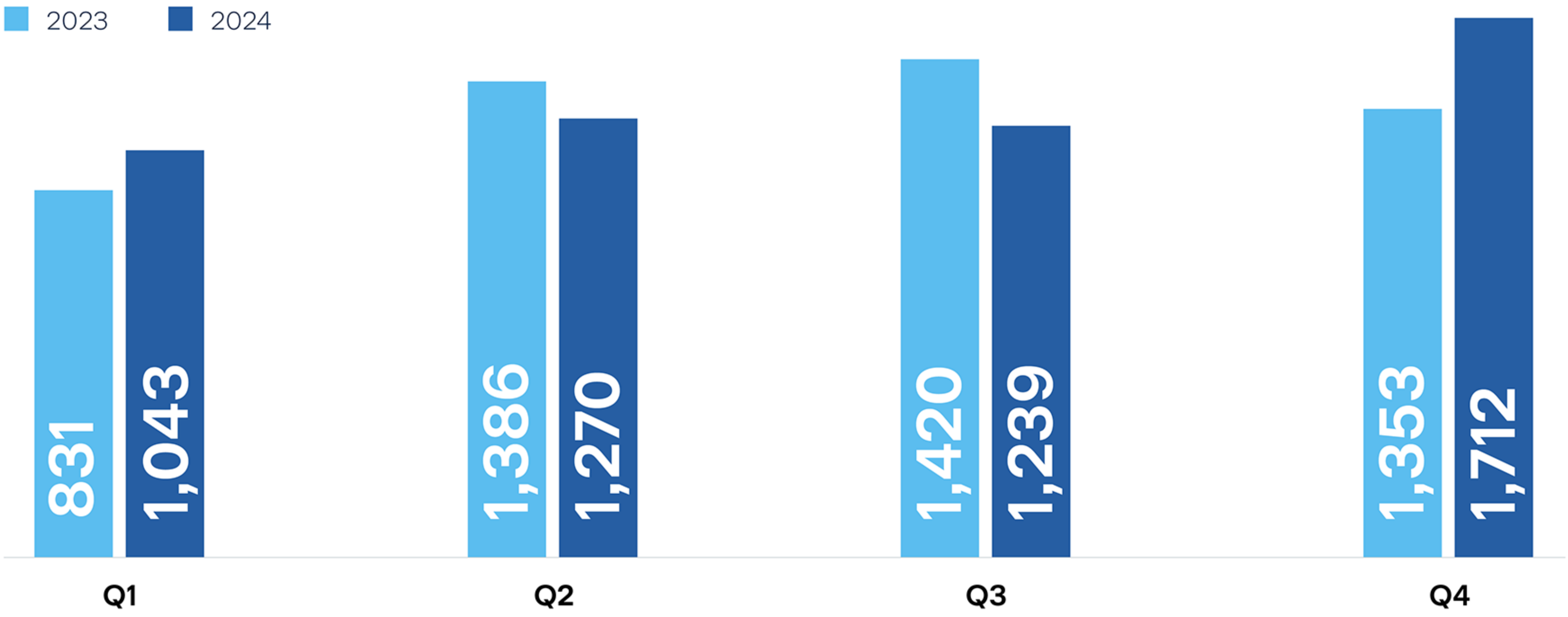
Email attacks are on the rise

- In H2 2024 the number of email-based attacks detected increased by 197%
- While the number of attacks per organization within the same time frame increased by 21%

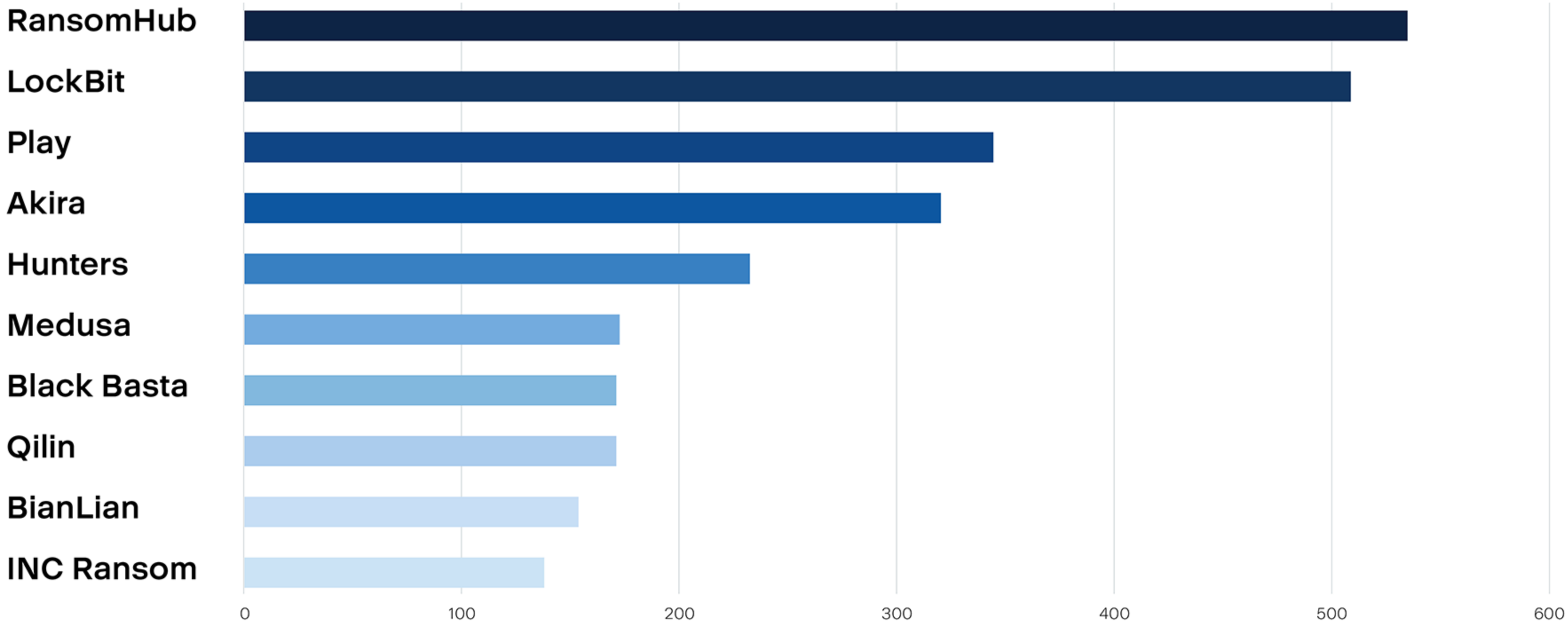
Number of ransomware cases is growing

Acronis

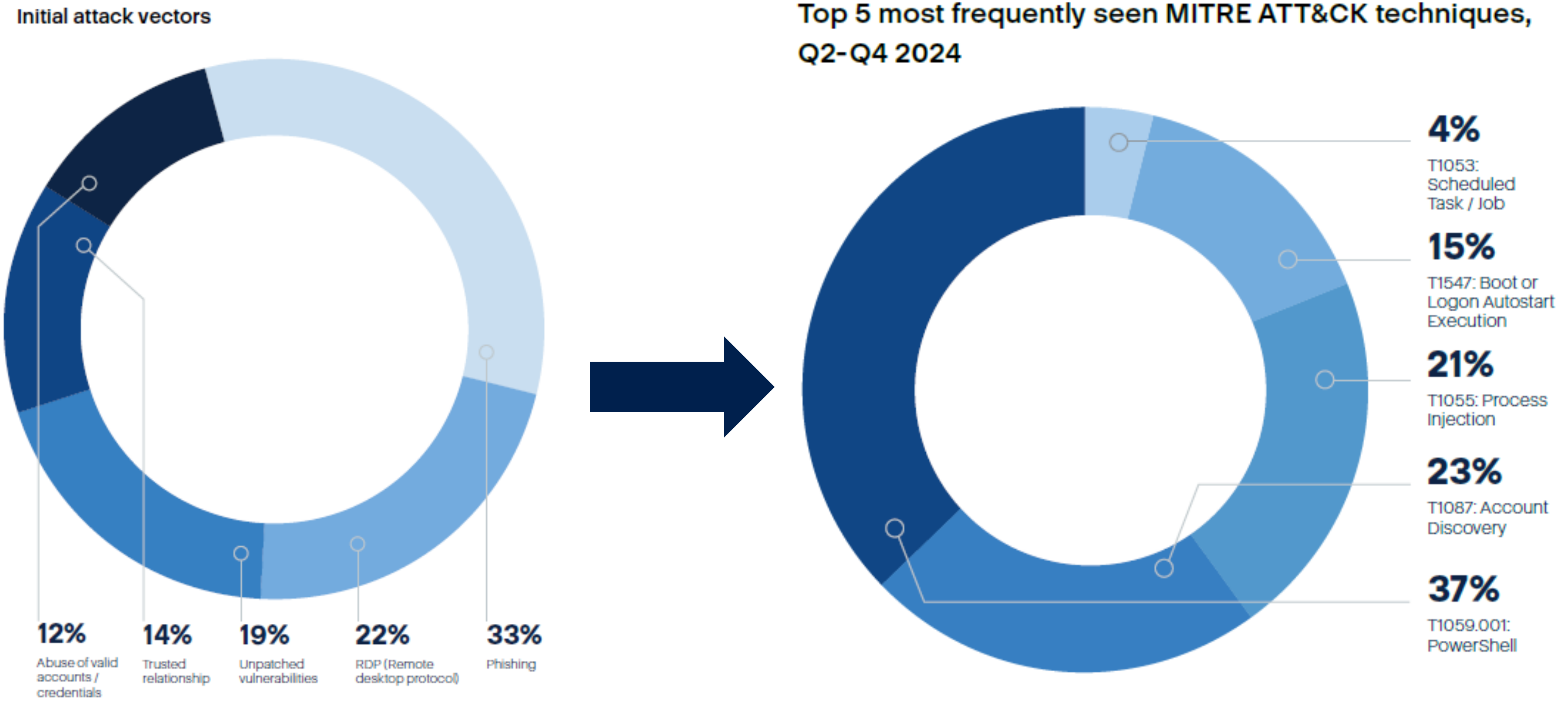
Cyberthreats Report, H2 2024



Top ransomware groups

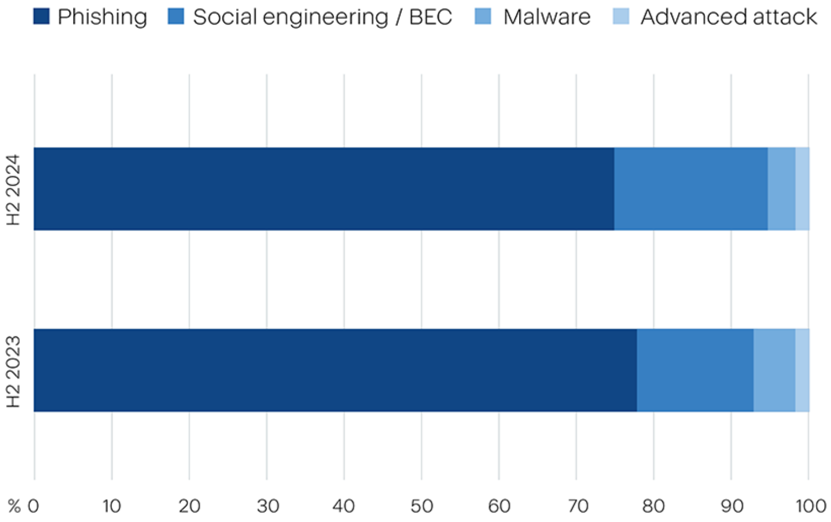


Main vectors and techniques of attacks on MSPs



Acronis

Social engineering attempts have increased 7% compared to one year ago



Total users attacked

47%

Monthly average

Phishing URLs

29%

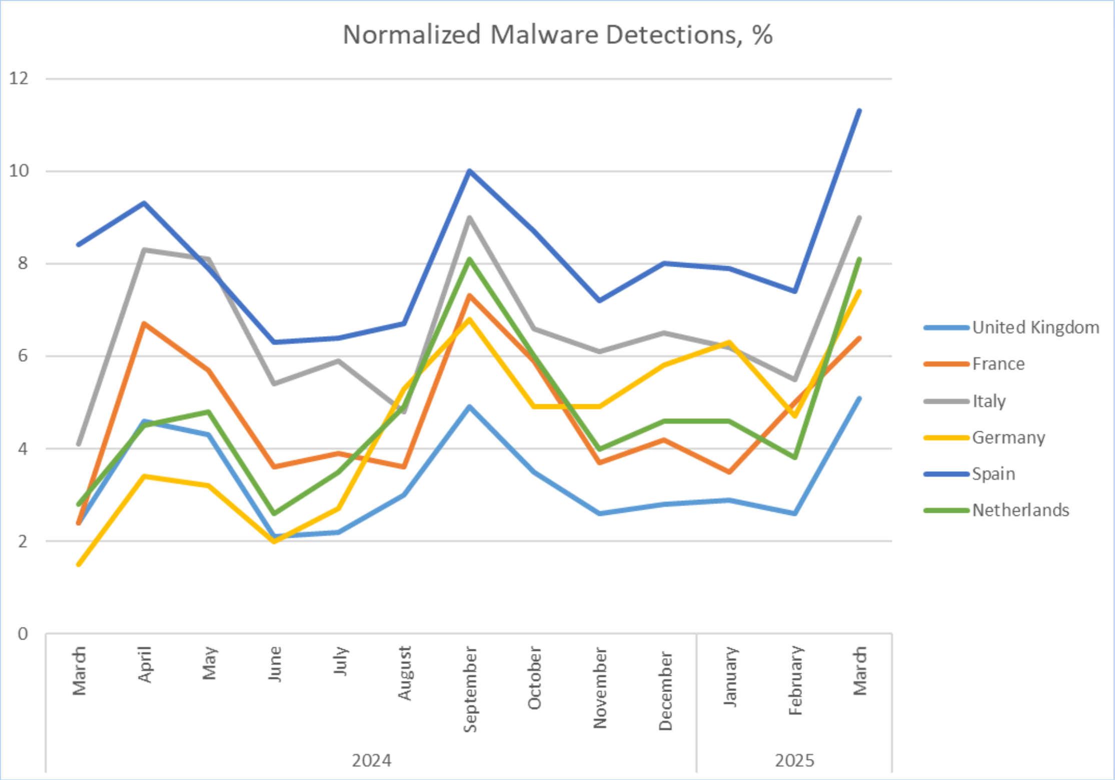
Monthly average

Files containing malware

14%

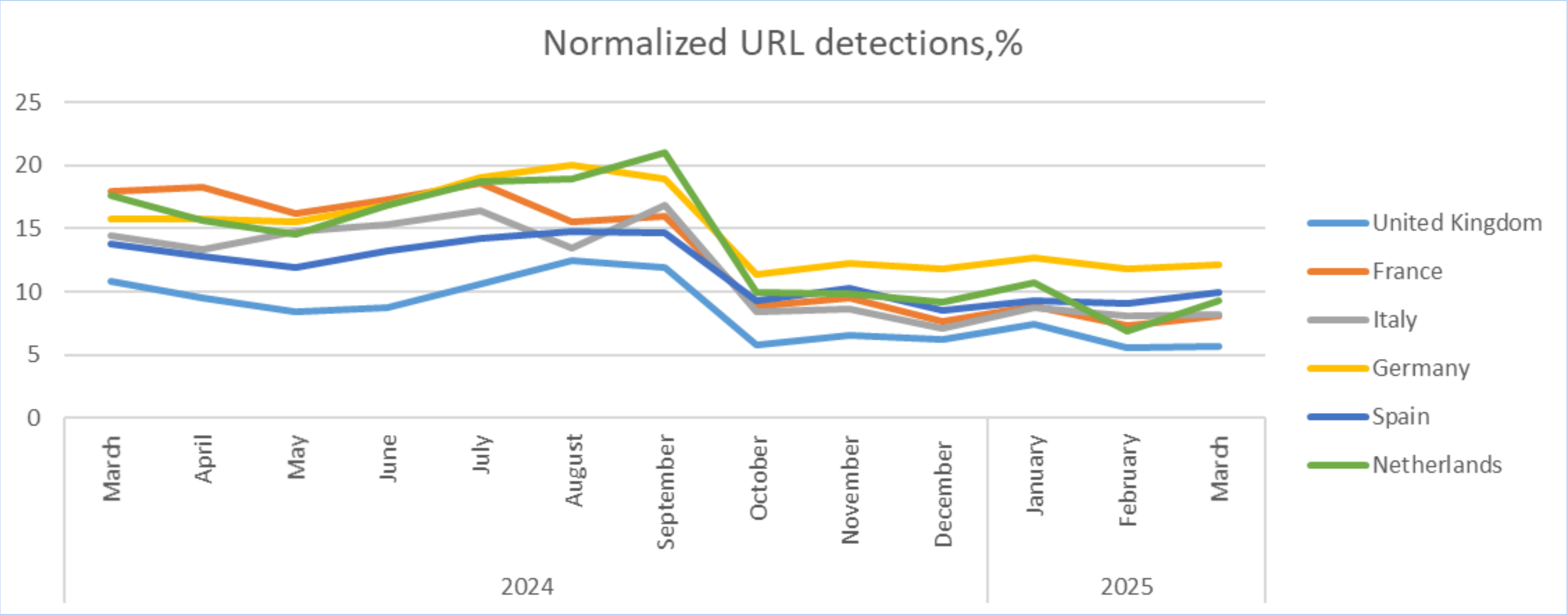
Monthly average

Malware detections in 2025*



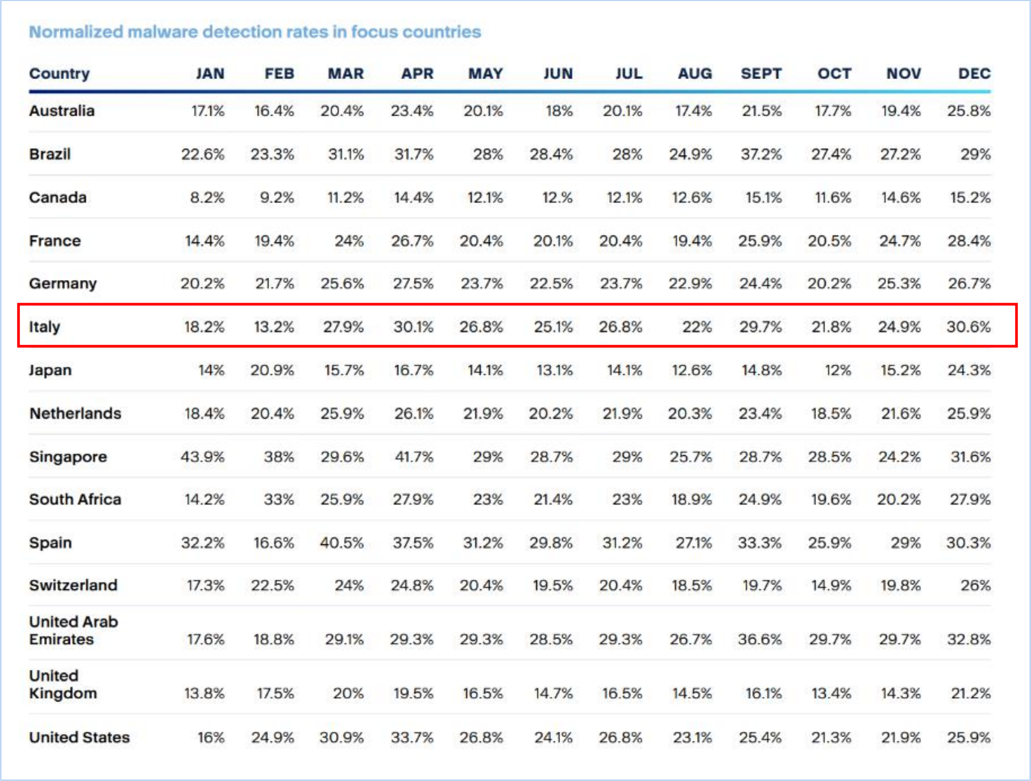
* New methodology

URL detections in 2025*



* New methodology

Malware detections in 2024



Normalized malware detection rates in focus countries

Country	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEPT	OCT	NOV	DEC
Australia	17.1%	16.4%	20.4%	23.4%	20.1%	18%	20.1%	17.4%	21.5%	17.7%	19.4%	25.8%
Brazil	22.6%	23.3%	31.1%	31.7%	28%	28.4%	28%	24.9%	37.2%	27.4%	27.2%	29%
Canada	8.2%	9.2%	11.2%	14.4%	12.1%	12.%	12.1%	12.6%	15.1%	11.6%	14.6%	15.2%
France	14.4%	19.4%	24%	26.7%	20.4%	20.1%	20.4%	19.4%	25.9%	20.5%	24.7%	28.4%
Germany	20.2%	21.7%	25.6%	27.5%	23.7%	22.5%	23.7%	22.9%	24.4%	20.2%	25.3%	26.7%
Italy	18.2%	13.2%	27.9%	30.1%	26.8%	25.1%	26.8%	22%	29.7%	21.8%	24.9%	30.6%
Japan	14%	20.9%	15.7%	16.7%	14.1%	13.1%	14.1%	12.6%	14.8%	12%	15.2%	24.3%
Netherlands	18.4%	20.4%	25.9%	26.1%	21.9%	20.2%	21.9%	20.3%	23.4%	18.5%	21.6%	25.9%
Singapore	43.9%	38%	29.6%	41.7%	29%	28.7%	29%	25.7%	28.7%	28.5%	24.2%	31.6%
South Africa	14.2%	33%	25.9%	27.9%	23%	21.4%	23%	18.9%	24.9%	19.6%	20.2%	27.9%
Spain	32.2%	16.6%	40.5%	37.5%	31.2%	29.8%	31.2%	27.1%	33.3%	25.9%	29%	30.3%
Switzerland	17.3%	22.5%	24%	24.8%	20.4%	19.5%	20.4%	18.5%	19.7%	14.9%	19.8%	26%
United Arab Emirates	17.6%	18.8%	29.1%	29.3%	29.3%	28.5%	29.3%	26.7%	36.6%	29.7%	29.7%	32.8%
United Kingdom	13.8%	17.5%	20%	19.5%	16.5%	14.7%	16.5%	14.5%	16.1%	13.4%	14.3%	21.2%
United States	16%	24.9%	30.9%	33.7%	26.8%	24.1%	26.8%	23.1%	25.4%	21.3%	21.9%	25.9%

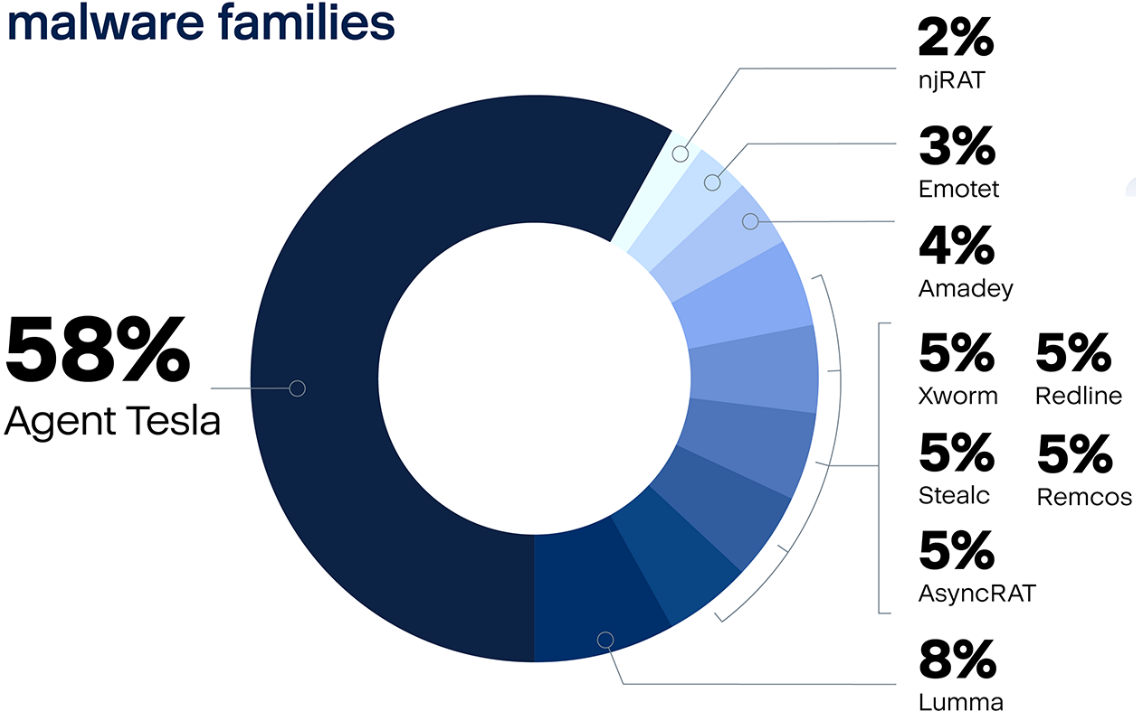
- Malware rates start at 18.2% (Jan) and peak at 30.6% (Dec). Peaks: March (27.9%), September (29.7%), and December (30.6%). Lows: June (25.1%) and July (26.8%), though still relatively high.

- Italy experiences sustained high malware activity, with the most significant threats occurring in March and December.

- Consistently high risk, requiring strong cybersecurity measures throughout the year.

Malware distribution globally and in Italy

Most commonly seen malware families



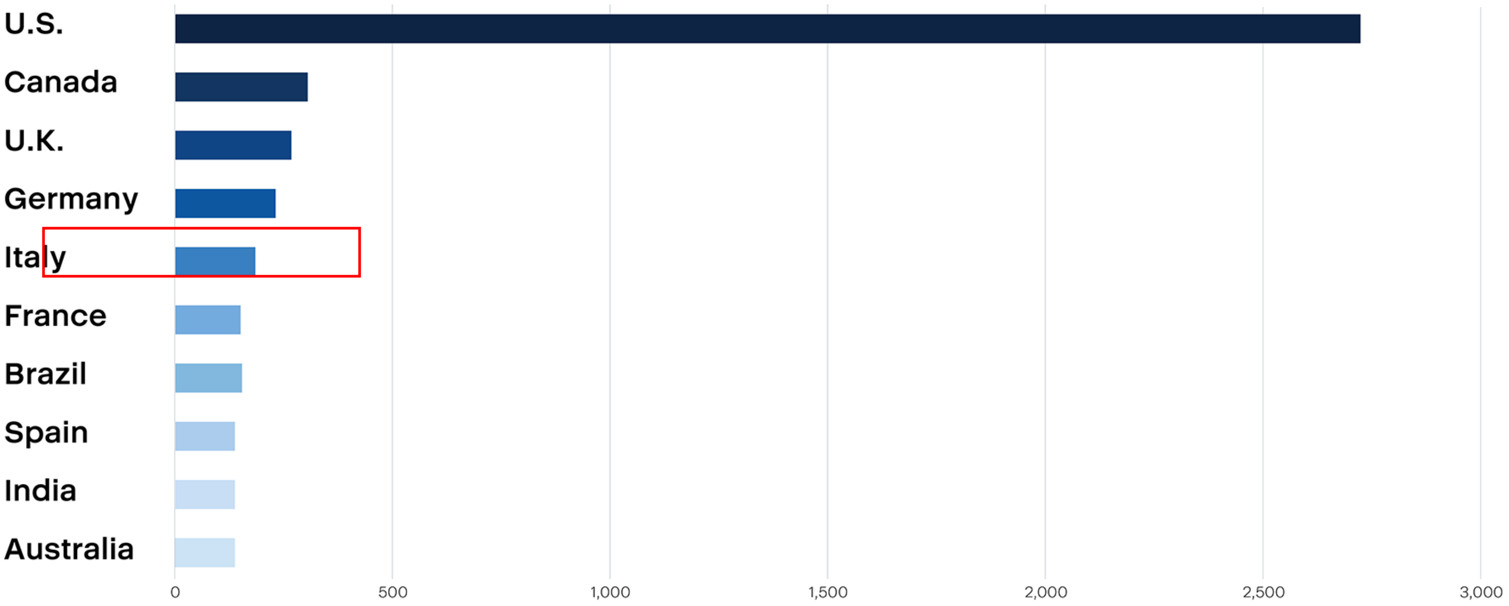
In 2024, we recorded a 50% increase in new variants, with an average of 289,000 new samples detected daily. Italy, Singapore, and the United Arab Emirates are among the most targeted countries.

In Italy: Infostealer Trojans like FormBook, Rhadamanthys, and AgentTesla dominate attack campaigns, spreading through phishing emails disguised as fake invoices, purchase orders, and legal documents to deceive victims.

Malware distribution is primarily via compressed archives (41%), followed by executable scripts (14%) and Office/PDF documents containing malicious links (10%), highlighting the evolution of attack techniques.

Ransomware Attacks Global Overview

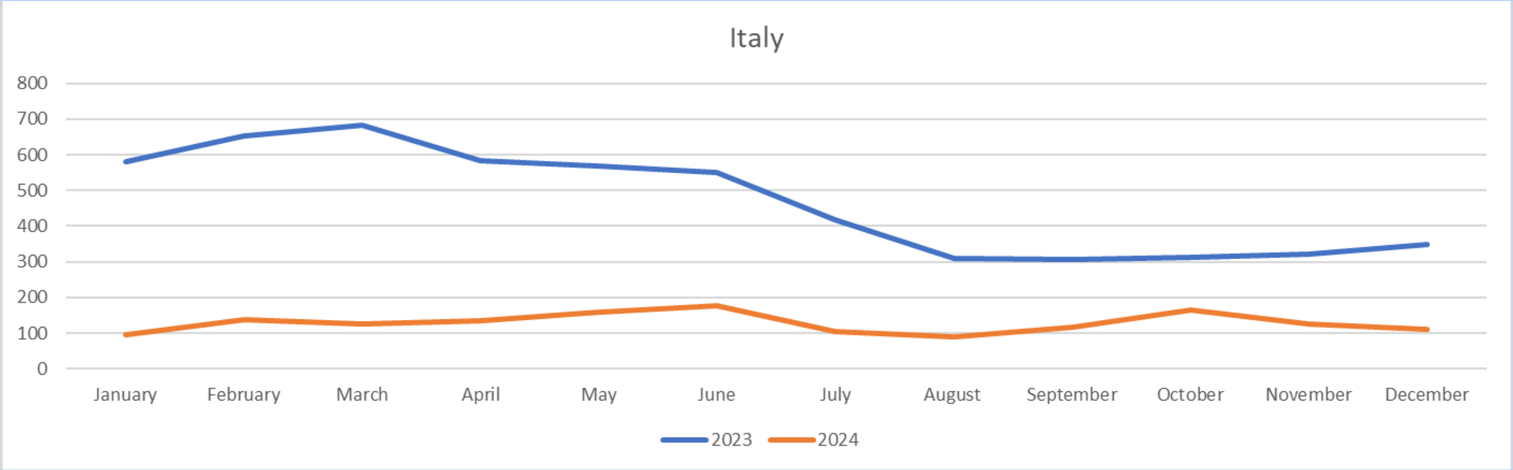
Top 10 countries for ransomware attacks



- 5th place with 146 attacks ;
- Total number of attacks in 2024 is 5264 worldwide;

- Ransomhub (18)
- Lockbit (12)
- 8base (11)
- Blackbasta (10) Akira (8)

Ransomware Detections telemetry data



Significant Decline from 2023 to 2024 – Ransomware detections in Italy have sharply decreased in 2024 compared to 2023, indicating improved cybersecurity defenses, law enforcement actions, or shifts in attacker strategies.

- In both years, ransomware activity declines from May to August, suggesting a seasonal trend where attacks slow down during summer, possibly due to vacation periods affecting both attackers and organizations.
- A minor increase in detections from September to December 2024 suggests that ransomware groups may still be exploiting holiday periods, but the scale is far smaller than in 2023.

Italy: Bio-Clima Service Srl Hit by Everest

Victim

- **Bio-Clima Service Srl** is specializing in technical assistance and maintenance for biomedical instrumentation
- **Industry:** Transportation
- **Revenue:** N/A

BioClimaLab SERVICES

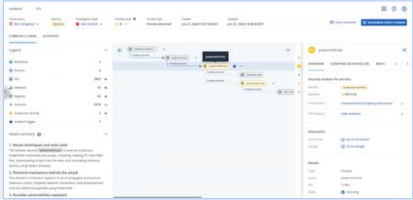
Threat vector and impact

- **Attacked by:** Everest, published on November, 15.
- **Attack vector:** through Initial Access Broker, selling unauthorized access to networks. Their tactics include lateral movement, credential access, and data exfiltration, often employing tools like Cobalt Strike for command and control communications.
- **Impact:** the group has shared sample screenshots of the stolen data, underscoring the severity of the breach.

How Acronis protects

- **Active Protection** inside core Acronis Cyber Protect detects and blocks any variant of Everest ransomware heuristically.
- **Product needed:** Acronis Advanced Security + XDR , Acronis Advanced Email Security.

Detection Screenshot



TRU Labs Statistics

*Malware detections:

24.9%

*Malicious URL was accessed:

8.9%

*normalized numbers, per unique machines in November 2024

Italy: Cosmed hit by Ransomware Attack

Victim

- **Cosmed** specializes in the global design, manufacturing, and distribution of diagnostic medical devices.
- **Industry:** Healthcare.
- **Revenue:** 42.8 M USD

COSMED
The Metabolic Company

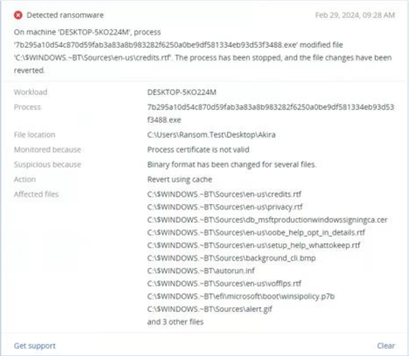
Threat vector and impact

- **Attacked by:** Akira, confirmed on February, 17.
- **Attack vector:** exploiting vulnerabilities in VPN services lacking multifactor authentication, as well as spear-phishing campaigns.
- **Impact:** 25 GB of essential corporate documents such as: passport scans, NDAs, confidential files, financial data (audits, payment details, reports), foreigner identity cards, etc.

How Acronis protects

- **Active Protection** inside core Acronis Cyber Protect detects and blocks Akira ransomware heuristically.
- **Product needed:** Acronis Advanced Security + XDR , Acronis Advanced Email Security.

Detection Screenshot



Detected ransomware Feb 29, 2024, 09:28 AM

On machine 'DESKTOP-5KO224M', process '7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488.exe' modified file 'C:\$WINDOWS.~BT\Sources\en-us\credits.rtf'. The process has been stopped, and the file changes have been reverted.

Workload: DESKTOP-5KO224M

Process: 7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488.exe

File location: C:\Users\Ransom.Test\Desktop\Akira

Monitored because: Process certificate is not valid

Suspicious because: Binary format has been changed for several files.

Action: Revert using cache

Affected files:
C:\$WINDOWS.~BT\Sources\en-us\credits.rtf
C:\$WINDOWS.~BT\Sources\en-us\privacy.rtf
C:\$WINDOWS.~BT\Sources\db_msftproductionwindowssigningca.cer
C:\$WINDOWS.~BT\Sources\en-us\oobe_help_opt_in_details.rtf
C:\$WINDOWS.~BT\Sources\en-us\setup_help_whattokeep.rtf
C:\$WINDOWS.~BT\Sources\background_cli.bmp
C:\$WINDOWS.~BT\autorun.inf
C:\$WINDOWS.~BT\Sources\en-us\vofflps.rtf
C:\$WINDOWS.~BT\efi\microsoft\boot\winsipolicy.p7b
C:\$WINDOWS.~BT\Sources\alert.gif
and 3 other files

TRU Labs Statistics

*Malware detections:

5.5%

*Malicious URL was accessed:

8.1%

*normalized numbers, per unique machines in February 2025

In today's challenging threat landscape, traditional security is not enough.

The need for EDR

Only advanced security can combat advanced attacks

More than 60% of breaches **involve hacking** (requires advanced and layered defenses).

EDR is associated with **a 58% reduction in serious security incidents**.

The need for EDR

Only advanced security can combat advanced attacks

More than 60% of breaches **involve hacking** (requires advanced and layered defenses).

EDR is associated with **a 58% reduction in serious security incidents**.

A breach is inevitable. You need to be prepared

>100 days to fully recover from a breach, including customer trust.

$4.88 million: Average total cost of a data breach — a 10% y/y increase.

70% of organizations experiences a “significant” or “very significant” disruption from the breach.

Sources: “Data Breach Investigations Report’, Verizon, 2024”; “Cost of data breach report”, 2024, IBM Security;

The need for EDR

Only advanced security can combat advanced attacks

More than 60% of breaches **involve hacking** (requires advanced and layered defenses).

EDR is associated with **a 58% reduction in serious security incidents**.

A breach is inevitable. You need to be prepared

>100 days to fully recover from a breach, including customer trust.

$4.88 million: Average total cost of a data breach — a 10% y/y increase.

70% of organizations experiences a “significant” or “very significant” disruption from the breach.

For many, compliance is mandatory

Regulations require organizations to **report security incidents** within a strict time-frame — e.g., 72 hours for GDPR, NIS2, US CIRCIA.

70% of breaches involve PII.

NIS 2

Sources: “Data Breach Investigations Report’, Verizon, 2024”; “Cost of data breach report”, 2024, IBM Security;

Acronis

TRU Security Day
Italy 2025

Italy

May 22, Milan

Acronis
Threat Research Unit