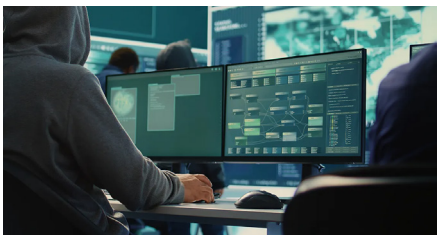
CyberGrant
SECURITY MADE EASY

WHITE PAPER

Ransomware, Spyware, and Backdoors: External Threats to Watch

Index

Cybersecurity landscape



Cybercrime is on the rise, and attacks are becoming increasingly sophisticated and costly. Organizations face growing challenges in protecting their systems, data, and operations.

Here are key statistics outlining the threat landscape as of 2025.

Global overview

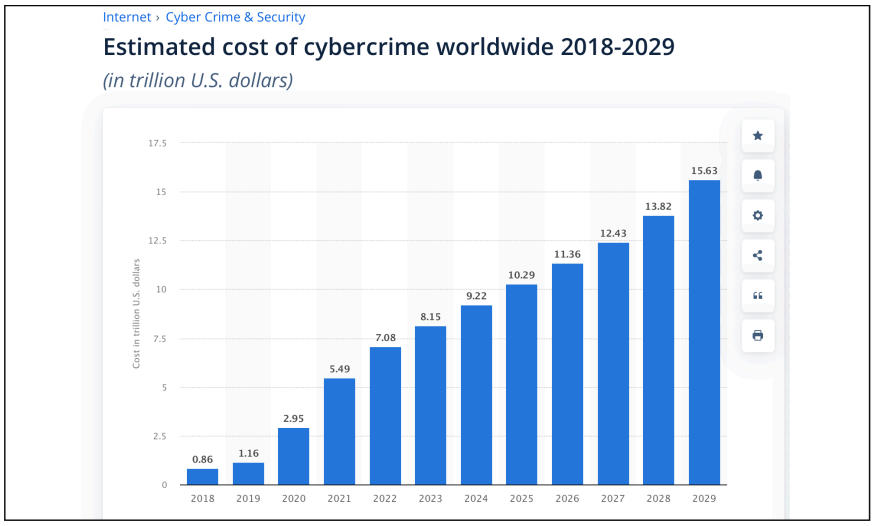


Image source: statista – technology market insight 2024

- Cybercrime is projected to **cost businesses up to $11.36 trillion by the end of 2025** and may reach $15.63 trillion by 2029. (Statista)
- The average cost of a **data breach globally** rose to approximately **$4.9 million in 2024** – a 10% increase over the previous year. One in three breaches involved shadow data. (IBM)
- **Ransomware incidents cost victims an average of $1.85 million per event,** with attacks increasing 13% over the last five years. (IBM)
- **Credential theft remains a critical issue**, with attacks using compromised credentials rising 71% year over year. (IBM)
- **A 17% rise in ransomware insurance claims in 2024**, with a 57% spike in Q4 compared to Q4 2023. (Deloitte)
- **60% of recipients fall for phishing emails generated by GenAI**, comparable to traditional phishing success

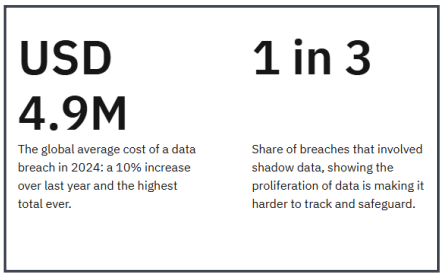


Image source: IBM Data Breach Report 2024

rates. (Harvard Business Review)

- Across industries, organizations take an **average of 204 days to detect and 73 days to contain a breach**. (IBM)
- Organizations that detect and **contain breaches within 200 days save $1 million** on average. (IBM)

Italy-specific data

Report: ACN operational summary – April 2025

- **118 ransomware cases recorded** – a 64% increase from the 72 incidents in the first four months of 2024
- **73 public ransomware claims by criminal group**s – up from 51 in the same period last year
- **24 ransomware attacks detected in April alone** – 30% more than in April 2024

Top attack vectors (April 2025):

- **Malicious email campaigns**
- Use of previously **compromised credentials**
- Exploitation of **known vulnerabilities**

16,957 potentially vulnerable assets – a 443% increase compared to Q1 2024

CLUSIT Cybersecurity Report – March 2025

- **Italy accounted for 10% of all global attacks in 2024**
- **3,577 severe** cyber incidents in 2024
- **+15% increase** in incidents over 2023

Distribution of attack techniques in Italy (2024):

- Malware: 38%
- DDoS: 28%
- Vulnerabilities: 19%
- Phishing/Social Engineering: 11%
- Unclassified Techniques: 7%
- Multiple Techniques: 2%
- Web Attacks: 2%

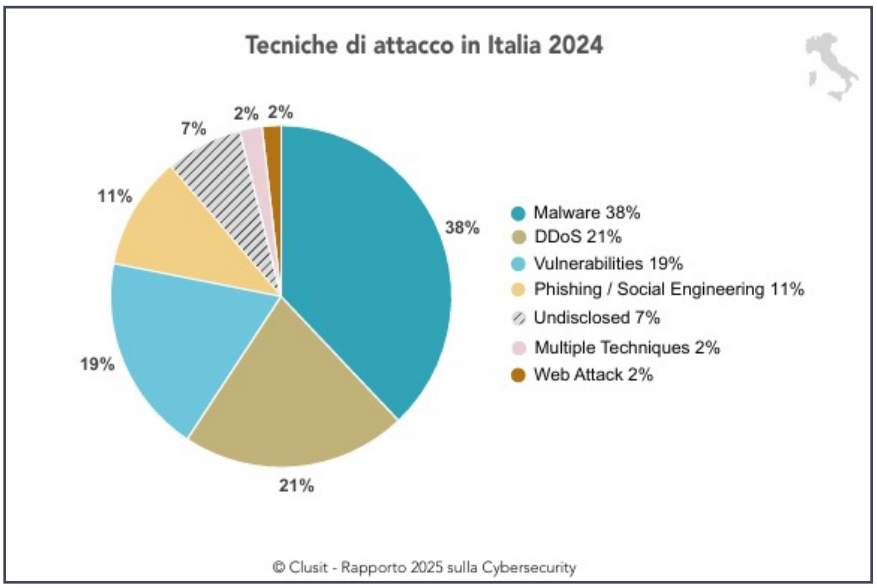


Image source: CLUSIT Cybersecurity Report 2025 – Distribution of Attack Techniques in Italy

Ransomware, spyware, and backdoors: what they are and how they work

Ransomware

Ransomware is a type of malware that prevents access to systems or files by encrypting them, followed by a ransom demand. In many cases, attackers exfiltrate data to increase pressure and force payment.

Ransomware has become the most visible and widespread form of malware, with high-profile cases crippling hospitals, halting city services, and damaging businesses.

Types of ransomware attacks

- **Double Extortion Ransomware –** Encrypts and steals data, threatening to publish it if the ransom isn't paid
- **Triple Extortion Ransomware –** Adds pressure via DDoS or direct extortion of customers or partners
- **Locker Ransomware –** Blocks access to the device rather than encrypting files
- **Crypto Ransomware –** Another term highlighting the use of cryptocurrencies in ransom payments
- **Wipers –** Permanently destroy access to encrypted files
- **Ransomware-as-a-Service (RaaS) –** Affiliates distribute malware, sharing ransom payments with developers

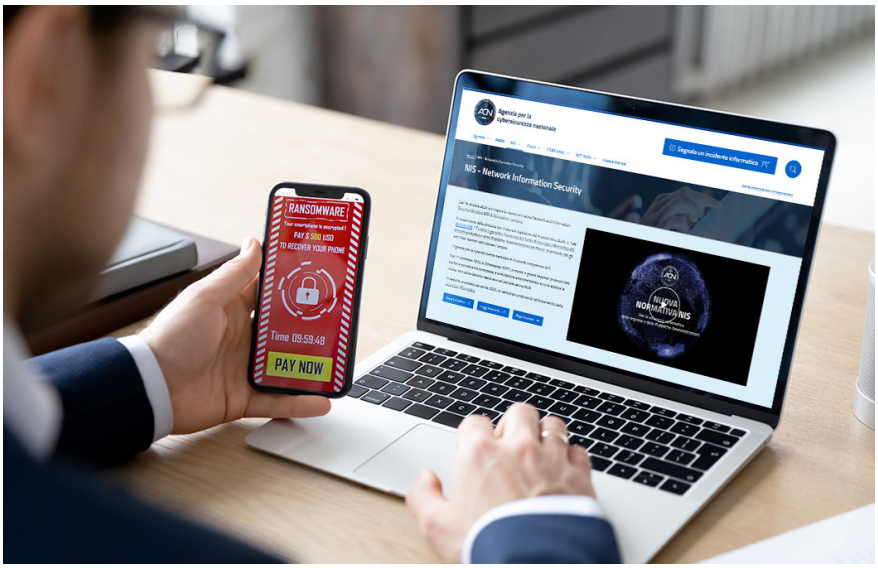
What to do after a ransomware attack

- **Isolate the Device** – Prevent lateral movement
- **Keep It Powered On** – Avoid data loss from sudden shutdowns
- **Back Up Encrypted Files** – In case future decryptors become available
- **Check No More Ransom** – A public-private initiative offering free decryptors
- **Seek Expert Help** – A forensic specialist may recover deleted backups
- **Wipe and Rebuild** – Reinstall OS from clean backups to ensure malware removal

Evolving legislation on ransom payments

Options for affected businesses:

1. **Report the breach and restore operations without engaging attackers**
2. **Report the breach but pay the ransom**
3. **Pay and conceal the breach**



International trends:

- **EU: NIS2 and DORA** mandate incident reporting and resilience
- **UK: Draft laws banning ransom payments** by critical infrastructure and government agencies
- **US: Federal and state-level restrictions** on large payments and delayed disclosures
- **Italy: Law 90/2024 introduces specific cyber incident management requirements;** additional legislation is under discussion

Spyware

Spyware is stealth malware that tracks user activity without consent. It captures:

- Browsing behavior
- Credentials
- Passwords
- Sensitive data

Attackers may use or sell this information for fraud, espionage, or extortion.

Common infection methods:

- Phishing emails
- Malicious downloads
- Fake apps
- Compromised websites

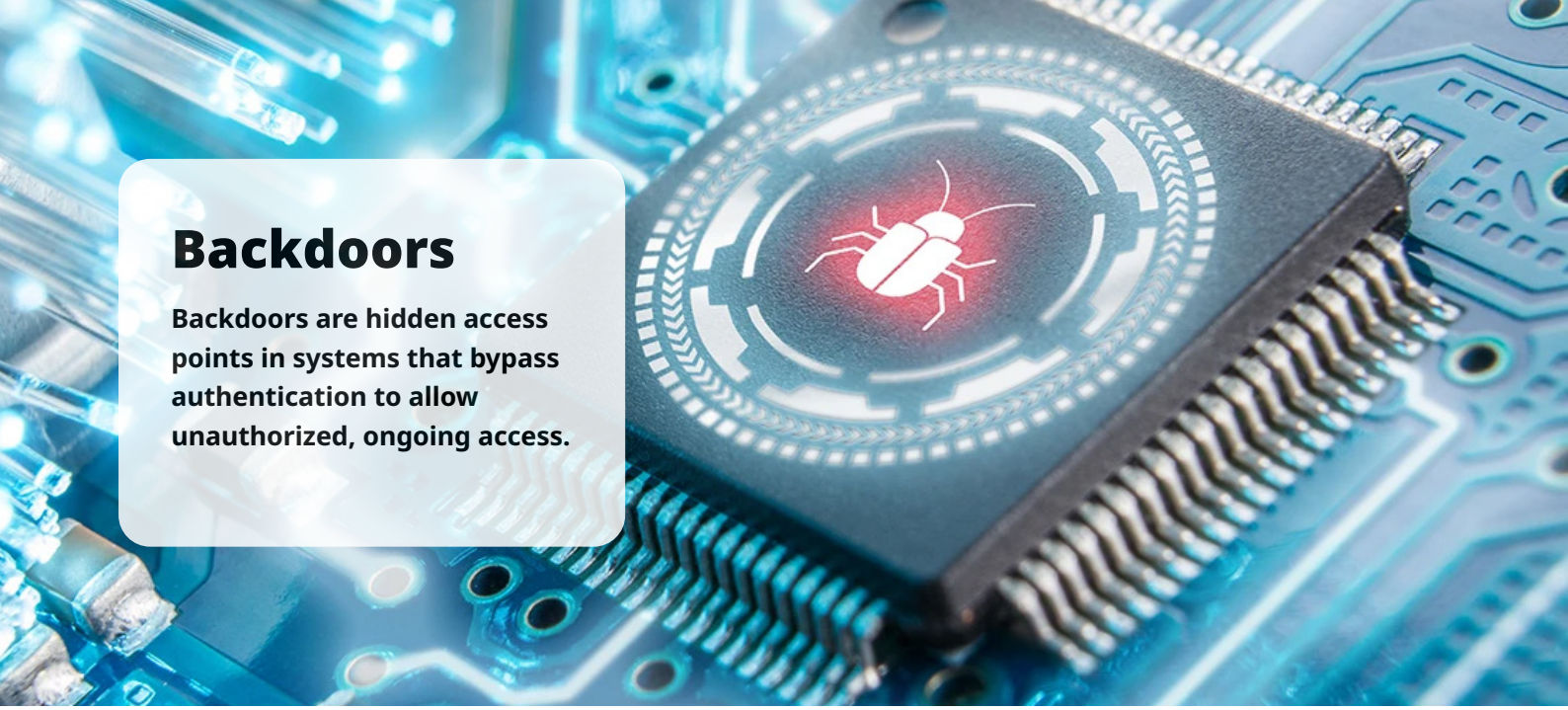
Types of spyware

- **Keylogger –** Records keystrokes, sends credentials to C&C servers
- **Spyware Trojan –** Delivered via malware disguised as legitimate software
- **Stalkerware –** Used for personal surveillance
- **Adware –** Injects ads; may open backdoors to other malware
- **Rootkits –** Hide spyware at kernel level, making detection extremely difficult

All internet-connected devices – PCs, Macs, iOS, Android – are potential spyware targets.

Spyware detection strategies

- Don’t interact with unexpected pop-ups
- Avoid unknown links or downloads
- Only install apps from trusted sources
- Be cautious with email attachments
- Use anti-spyware tools



Backdoors

Backdoors are hidden access points in systems that bypass authentication to allow unauthorized, ongoing access.

They're typically introduced through:

- Malware
- Phishing
- Unpatched vulnerabilities
- Compromised software/hardware supply chains

Once active, they can persist undetected for months or years, enabling data theft, sabotage, or further attacks.

Backdoor infection vectors

- **Malware Installation –** Often hidden in fake apps or files
- **Network Exploits –** Injected into routers/firewalls to intercept traffic
- **Social Engineering –** Steals credentials to silently install backdoors
- **Supply Chain Compromise –** Malicious code embedded during manufacturing

Signs of a backdoor attack

- **Unusual system lag** – background processes consuming resources
- **Anomalous network traffic** – Especially outbound to unknown IPs
- **Unexpected configuration changes** – admin rights, firewall rules, etc.
- **Crashes or instability –** deliberately triggered to hide malicious actions

Common types of backdoor attacks

- **Rootkits** – Kernel-level tools used in APTs, invisible to standard AV
- **Trojan Horses –** Fake apps installing secret access channels
- **Application-Level Backdoors –** Operate within trusted software
- **Hardware-Based Backdoors –** Embedded in physical components
- **Network-Based Backdoors –** Modify traffic through compromised devices
- **Cryptojacking –** Exploits system resources for illicit cryptocurrency mining

Consequences of ransomware, spyware, and backdoor attacks

Direct consequences

- **Data Theft –** Intellectual property, customer records, financials
- **Business Disruption** – System outages, halted operations, delivery delays
- **Financial Loss** – Incident response, ransom payments, fines, recovery costs
- **Reputation Damage** – Lost customer trust, investor concerns, competitive loss
- **Legal and Regulatory Risk –** GDPR, NIS2, DORA violations; lawsuits; compliance upgrades
- **Botnet Participation** – Compromised systems used to attack other entities

Best practices to prevent these attacks

Routine security controls

- Conduct regular audits and system scans
- Use SIEM and SOAR tools for behavior analysis

Intrusion detection and threat monitoring

- Deploy IDS/IPS and EDR tools
- Monitor for lateral movement or data exfiltration

Endpoint protection

- Use AI/ML-enhanced antivirus and antispyware solutions
- Detect ransomware, spyware, and unauthorized backdoor installation

Employee awareness

- Train staff on phishing, password hygiene, and suspicious behavior reporting
- Simulate attacks to build a security-first culture

Timely patching

- Apply updates promptly
- Enable auto-updates where feasible
- Replace outdated hardware/software

Access control

- Use RBAC and MFA
- Implement Zero Trust principles
- Deploy DLP systems to block unauthorized access attempts

Isolated backups

- Backup critical systems daily
- Store backups offline or segmented
- Test restoration processes regularly

Mobile and desktop spyware protection

- Scrutinize app permissions
- Block pop-ups
- Install only verified apps

Real-Time threat detection

- Partner with MSSPs for 24/7 monitoring
- Use proactive detection tools to spot ransomware and spyware early

CyberGrant supports prevention with RemoteGrant

RemoteGrant

CyberGrant Inc. helps organizations strengthen cybersecurity defenses with its **RemoteGrant platform**, designed to:

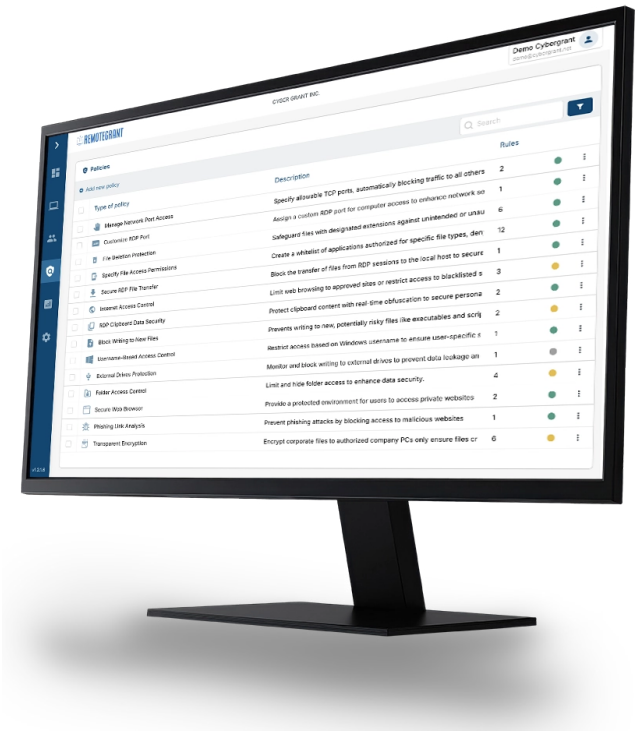
- Monitor and detect suspicious activity on endpoints
- Encrypt company files and limit access to authorized apps/ devices
- Alert on anomalies and block ransomware, spyware, and backdoor threats
- Provide real-time exploit and vulnerability protection
- Control and log remote access
- Capture detailed logs for forensic analysis
- Enforce multifactor authentication (MFA)

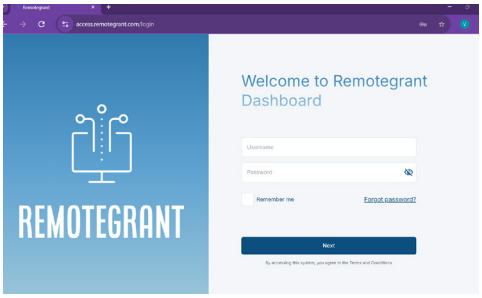
RemoteGrant helps ensure compliance with data protection and privacy regulations, including GDPR, NIS2, and DORA.

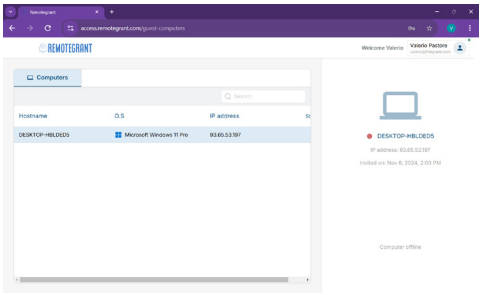
Advantages of RemoteGrant

It also allows businesses to:

- **Restrict apps allowed to access sensitive data**
- **Prevent copy/paste/export of protected files**
- **Define file extensions eligible for protection**
- **Limit protection to specific computers**
- **Block remote file transfers via RDP**
- **Prevent writes to secure folders to stop tampering**







Conclusion

As cyber threats grow in scale and sophistication—especially ransomware, spyware, and backdoors—businesses must shift from reactive to proactive.

Understanding internal vulnerabilities is the foundation of a resilient cybersecurity strategy. Building this awareness enables prevention, detection, and rapid response.

Continuous investment in training and simulation exercises builds organizational muscle and improves readiness in crisis scenarios.

Adopting cybersecurity, business continuity, and risk management in a unified, risk-based strategy is not just a regulatory necessity—it's a competitive advantage.

In today's threat environment, resilience isn't optional. It's essential.

Edited byi **Federica Maria Rita Livelli**

www.cybergrant.net