
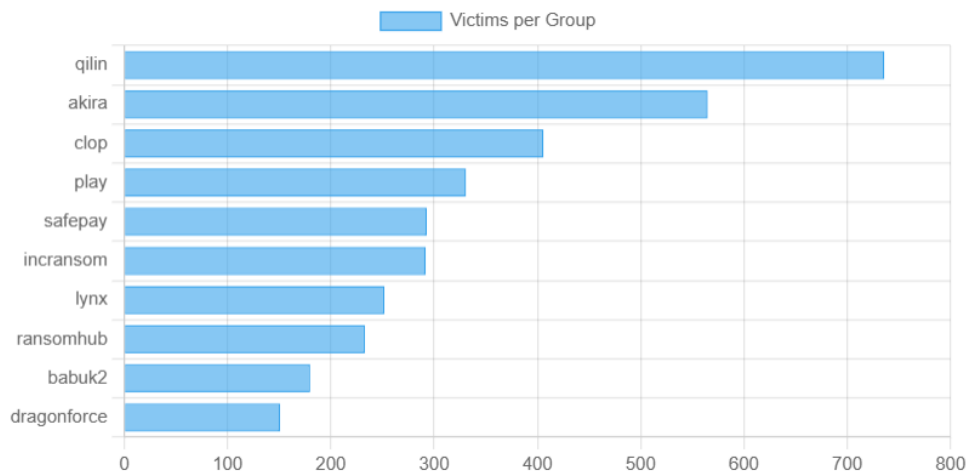


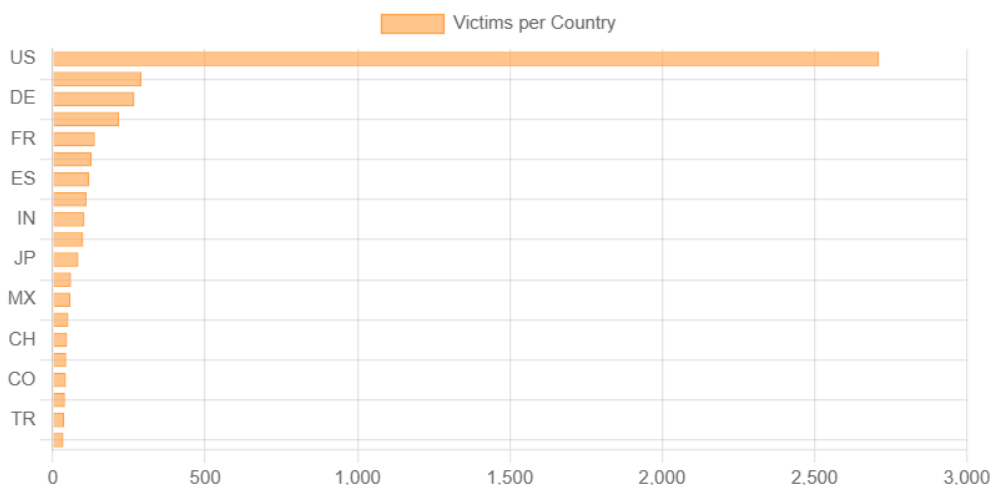
Ransomware Incident Response Playbook

Ransomware has evolved from being opportunistic attacks to highly sophisticated operations that can cripple an organization within hours. These attacks not only encrypt critical files but also threaten operational continuity and can have severe financial and reputational consequences. A well-crafted ransomware playbook helps teams respond quickly, limit damage, recover systems safely, and learn from the incident to prevent future attacks. This guide outlines detection, containment, eradication, recovery, and post-incident actions, with practical advice for real-world implementation. Below are some statistics provided by [Ransomware.live](https://ransomware.live) 

Top 10 Groups



Top 10 Countries



Detection Phase

Detecting ransomware early is essential to limit its impact. SOC teams should monitor for several warning signs. These include sudden mass changes to files with unusual extensions such as .encrypted, .locked, or .crypto. Unusually high CPU or disk usage can indicate active encryption processes. Deletion of system backups or shadow copies is another red flag. Communications with known command and control servers should trigger immediate investigation. Suspicious scripts, especially in PowerShell or WMI, may also point to ransomware deployment.

Effective monitoring requires a combination of endpoint detection, network traffic analysis, email gateway inspection, and cloud storage oversight. Alerts must be validated carefully to avoid false positives, which could disrupt normal business operations unnecessarily. Regularly updating detection rules with intelligence from past incidents and threat feeds ensures that SOC teams stay ahead of evolving ransomware tactics.

Containment Strategies

Once ransomware activity is confirmed, the next step is to contain it. The strategy depends on the scale of the infection. For localized incidents, affected devices should be immediately disconnected from the network. Implementing temporary network segmentation prevents the ransomware from spreading to other systems. File-sharing services and mapped drives should be disabled to avoid encrypting additional data. Backups should be temporarily suspended to protect them from infection. If critical systems are being actively encrypted, emergency shutdown procedures may be necessary.

For broader infections, containment decisions become more complex. SOC teams need to assess whether isolating segments of the network is sufficient or if a full network shutdown is necessary. These decisions must balance the urgency of stopping the attack with the need to maintain critical business functions. Coordination with IT management, legal teams, and executives ensures informed decisions are made quickly. All containment steps should be thoroughly documented for accountability and future analysis.

Eradication and Recovery

Eradication focuses on removing the ransomware from the environment and preventing reinfection. All affected machines should be preserved for forensic analysis to understand attack vectors and the attacker's methods. Any malware remnants, backdoors, or persistence mechanisms must be removed. Systems should be rebuilt using clean images or validated configurations. Data should be restored from offline or air-gapped backups whenever possible. Before reconnecting restored systems, verification checks must confirm they are free of malware.

Recovery prioritization should follow business criticality. Systems essential for operations are restored first, followed by non-critical devices. Testing each restored system ensures that business processes can resume safely. Legal and management teams should be consulted regarding ransom payment decisions. If payment is considered, a controlled and documented procedure should be followed to acquire cryptocurrency and communicate with negotiation specialists securely.

Post-Incident Activities

Once systems are restored, post-incident actions are crucial for organizational learning. Evidence should be preserved for regulatory or legal purposes. Root cause analysis helps identify how the ransomware entered the environment and what security gaps were exploited. SOC teams should evaluate the effectiveness of existing controls and identify areas for improvement. Debrief sessions with all stakeholders ensure lessons are shared across teams. Playbooks, policies, and controls should be updated based on these insights.

Additionally, organizations should implement employee awareness programs to reinforce safe practices, such as recognizing phishing emails and avoiding suspicious links or attachments. These efforts reduce the likelihood of future ransomware incidents and strengthen overall security culture.