

CISA and partners: SafePay ransomware has hit over 600 critical infrastructure organizations



CISA and partner agencies report that SafePay ransomware has affected at least 600 critical infrastructure organizations since August 2024, mainly via exposed credentials, brute force and VPN access, and unpatched edge devices.

- SafePay has affected at least 600 critical infrastructure organizations across several sectors since August 2024.
- Initial access comes from exposed credentials, brute force attacks, VPN access, phished accounts and exploited edge-device vulnerabilities.
- Attackers may delete shadow copies and reset network-attached storage holding backups to hinder recovery.
- The group uses double extortion and operates privately, without affiliates.

- The joint advisory includes IOCs and TTPs and warns that paying a ransom does not guarantee file recovery.

The US Cybersecurity and Infrastructure Security Agency (CISA), together with the FBI, the US Secret Service, Germany's Landeskriminalamt Rheinland-Pfalz and UK law enforcement bodies, has published a joint advisory on the **SafePay** ransomware group. It says the group has affected at least 600 organizations across multiple critical infrastructure sectors since August 2024, with victims in North America, South America, Europe and Australia.

How the attacks work

The advisory lists several routes to initial access: exposed credentials, brute force password attacks, VPN access, phished account profiles, and automated exploitation of known vulnerabilities in edge devices and other internet-exposed systems. After gaining access, the actors may delete shadow copies and reset network-attached storage devices that hold backups, which complicates recovery. SafePay also steals sensitive documents before encryption and threatens to publish them if no ransom is paid.

The group emerged in August 2024 and works privately, without affiliates. Its leak site only lists victims who did not pay, so the real number of victims is higher than the public count.

What the agencies recommend

The authors advise restricting administrative tools and privileges to limit lateral movement, enforcing multifactor authentication and identity, credential and access management policies, and prioritizing updates for VPNs, firewalls and other edge devices that appear in CISA's catalog of actively exploited vulnerabilities. They add that paying a ransom does not guarantee recovery of files and encourage victims to report incidents to law enforcement. The advisory also includes indicators of compromise and tactics, techniques and procedures drawn from investigations of activity between November 2024 and August 2026.

The source does not report specific activity in Saudi Arabia or the Gulf, but the access methods described apply to any organization with exposed remote access.

What to do now

1. Review VPN, firewall and other internet-facing devices and prioritize patching those listed in CISA's known exploited vulnerabilities catalog.
2. Enforce multifactor authentication on remote access and privileged accounts, and check for exposed or reused credentials and brute-force attempts in VPN logs.
3. Restrict administrative tools and privileges to limit lateral movement after a compromise.
4. Protect backups: keep offline or immutable copies, restrict access to NAS devices, and monitor for shadow copy deletion.

5. Load the advisory's IOCs and TTPs into detection tooling and hunt for related activity.
6. Update the ransomware response plan, including reporting to the National Cybersecurity Authority and other relevant authorities.