

CHOSEN BRICK: UK, US and Dutch agencies warn of Iranian malware aimed at dissidents and journalists



The UK NCSC, FBI and Dutch AIVD describe CHOSEN BRICK, a Windows malware spread through social engineering on messaging apps, which can reach personal as well as corporate devices.

- CHOSEN BRICK has been used since at least 2025 against individuals in the UK, US and the Netherlands.
- Attackers build rapport on WhatsApp or Telegram, posing as known contacts or platform support, then push a fake application or file.
- The malware runs on Windows, persists through a registry Run key, adds Microsoft Defender exclusions and uses Telegram for command and control.
- It can capture screens and audio, copy Telegram and WhatsApp browser data and steal email; no automated lateral movement has been observed.

- Attackers move from corporate to personal devices when delivery fails, so organisations should help staff check both.

The UK National Cyber Security Centre, the US Federal Bureau of Investigation and the Netherlands' AIVD have published a joint advisory on CHOSEN BRICK, a malware family used by Iranian state cyber actors. The agencies say it has targeted individuals in several countries since at least 2025, mainly dissidents, activists and journalists. Personal details of some earlier victims have appeared on pro-Iranian leak sites.

How the attack works

The actors research their target, then approach through messaging platforms such as WhatsApp and Telegram, posing as someone the target knows or as platform technical support. The target is persuaded to open a file that looks genuine, such as a well-known application or, in some cases, MRI scan results. A convincing screen is shown while the malware installs in the background. Contact often starts on a work device; if that fails, the actor asks the person to open the file on a personal device to avoid corporate controls.

Once installed on Windows, the malware survives reboots through the HKCU Run registry key, adds exclusions to Microsoft Defender and uses a separate Telegram bot for each victim. It can capture the screen and microphone, copy Telegram and WhatsApp data from browsers, steal email and download further malware. Data leaves via Telegram and cloud storage services. No automated lateral movement has been observed.

Detection and mitigation

The advisory advises organisations that suspect execution to have IT teams search logs for the published indicators and run the detection signatures. Unexpected DNS or proxy connections to api.telegram.org, backblazeb2.com, vultrobjects.com, storjshare.io, iproyal.com and lightningproxies.net deserve review. Staff likely to be targeted should be told and helped to check personal devices as well. The recommended controls are phishing-resistant MFA, application allowlisting, antivirus, email scanning, endpoint and network monitoring, and user awareness training.

What to do now

1. Search DNS and web proxy logs for the listed domains and review unexpected connections, especially to api.telegram.org.
2. Check endpoints for the HKCU Run registry entries and the non-standard 'Windows ' (trailing space) SysWOW64 path described in the advisory, and run the published detection signatures.
3. Alert staff at higher risk, such as executives and media or public-affairs teams, and offer help checking personal devices.
4. Enforce phishing-resistant MFA, application allowlisting and managed antivirus, and alert on Microsoft Defender exclusion changes.

5. Add lures posing as messaging-app support or software installers sent over WhatsApp or Telegram to awareness training.
6. Report confirmed incidents under your internal process and to the National Cybersecurity Authority as required.