Iranian cyber targeting of dissidents, activists and journalists

Advisory on CHOSEN BRICK malware, including technical analysis and advice to help individuals and organisations protect themselves.

Introduction

CHOSEN BRICK is a malware family that has been used to target individuals around the world including in the UK, US and the Netherlands from at least 2025. CHOSEN BRICK enables Iranian state cyber actors to collect information on a target's contacts, emails and social media messages, which could enable tracking of their movements.

Iran almost certainly uses cyber activity to support the repression of individuals who are seen as a threat to the regime, such as dissidents, activists and journalists. In some cases, the Iranian intelligence services have plotted to kidnap or conduct lethal operations against individuals internationally, who they perceive as enemies of the regime.

The personal details of some previous victims of CHOSEN BRICK have appeared on pro-Iranian leak sites, potentially increasing the risk to the personal safety of those affected.

This advisory from the UK National Cyber Security Centre, the US Federal Bureau of Investigation and the Netherlands' General Intelligence and Security Service - Algemene Inlichtingen- en Veiligheidsdienst (AIVD) shares technical information about the malware, TTPs, as well as advice to help individuals and organisations.

Attack chain analysis

The Iranian cyber actors tailor their approach to their intended target and as such there is a wide variation in the initial approach to the target. There is also variation in the intended outcome of their operations. The core pattern of the actors' attack chains consists of:

- Initial contact and access via social engineering of the target via social messaging platforms, such as but not limited to WhatsApp and Telegram, purporting to be trusted entities.
- The malicious payload is disguised to match the social engineering approach and appear authentic to the target.
- The malicious payload deploys additional malware leveraging Telegram for command and control to blend in with legitimate processes.
- The malware has a wide range of functionality, enabling it to be used flexibly to support a range of potential operational outcomes.

Delivery and exploitation

Iranian cyber actors engaged with targets via social messaging applications to build rapport prior to attempting to deliver the malware. The nature of the social engineering varies between targets and uses extensive target knowledge from research conducted in preparation (T1589). The actor often purports to be an individual previously known to the target or technical support from the social messaging platform (T1566.003).

The actor uses this rapport with the target to convince them to download and open a file that appears authentic to the target (T1204.002). These have been in the form of applications appearing to be legitimate applications such as Pictory, RunwayML, Norton Antivirus, Telegram, Adobe Flash Player and KeePass. In other instances, they have been files appearing to be MRI scan results.

The actor often initiates contact with the target's work-related or corporate device in the first instance. If the initial delivery fails or the risk of detection is deemed significant, the actor will attempt to transition the delivery to personal devices by asking the target to open the file on their own devices, evading corporate security controls that protect the individual.

Regardless of the file thematic, the approach has been to display a legitimate appearing screen to the target fitting with the thematic to maintain the deception. In the background, the file also downloads and runs a core malware component (tracked by the NCSC as CHOSEN BRICK) enabling control over the target's device. In all observed instances, the malware has been exclusively targeted at the Windows operating system.

An example of the lure files once open are below:

Installation

CHOSEN BRICK is persistent and will survive a reboot of the target device. To do this it uses registry keys (T1547.001), most often the Run key in "**HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Run**". This will run the malware at user login for the user that was logged in when the malware was installed.

CHOSEN BRICK adds exclusions to Microsoft Defender antivirus in an attempt to evade detection (T1685).

Once established on the victim, the malware connects to Telegram for Command and Control (T1102.002). Each victim device connects to a different Telegram Bot ID unique to them as an Operational Security precaution, preventing cross-contamination between victims.

The malware has not been observed to have automated lateral movement capabilities and has focused on single devices. It has, however, been observed downloading additional malware and setting up persistence for the new payload with the same registry key it uses for its own persistence. As it can download additional malware, it is technically possible to enable lateral movement although this has not been observed.

Action on objectives

The CHOSEN BRICK malware family has a wide variety of in-built commands, as well as the ability to run commands through the native tools built into Windows. Through the Telegram bot, the malware can be tasked with a variety of functions including, but not limited to:

- Enumerating running processes (T1057) and system information (T1082)
- Capturing screen content (T1113)
- Enabling the microphone to capture audio content (T1123)
- Capture a copy of Telegram and WhatsApp data from web browsers (T1005)
- Download additional files enabling the use of further malware
- Delete files (T1485)
- Steal email content (T1114.001)
- Wipe the computer system (T1485)

Screen capture is a data theft feature commonly observed in these infections (T1113). This data can be used by the actor to identify the victim's contacts, location and pattern of life.In some circumstances the Iranian cyber actors have chosen to publish personal details retrieved in this way in order to further harass the victim.

Files and collected data are exfiltrated through a combination of the Telegram bot (T1041) and through the use of cloud object stores such as VultrObjects and StorjShare (T1567.002). Recent variations in this malware family include the use of HTTPS/SOCKS5 proxies to obscure the use of Telegram bots (T1090.002).

If the malware is instructed by the cyber actor to download additional malware it is written to disk in a configurable location. The most common observed is "C:\Windows \SysWOW64". In at least one sample, there was functionality for data wiping (T1485). NOTE: there is a space after "Windows" making this a non-standard location on most Windows devices, specifically created by the actor for the purpose of deploying malware.

Investigating potential compromise

Organisations that are concerned CHOSEN BRICK has been executed should contact their IT providers, either internal or external, to investigate. This investigation should include, but not be limited to, searching available logging for the IOCs provided, looking for evidence of CHOSEN BRICK as mentioned in the Installation, and Action on objectives sections of this document, and running the detection signatures provided. As this actor targets personal devices, not just corporate devices, organisations are recommended to circulate this with their staff that are likely to be targeted and support them in checking their personal devices too.

Check for persistence

The registry path "**HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Run**" contains programs configured to run automatically when the current user logs in. Malware commonly abuses this location because:

- It does not require administrative privileges.
- Entries run automatically on each logon.
- Users rarely inspect these values.

To check programs currently configured to start in this way, individuals can use the built in regedit tool or run the powershell command:

reg query HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Run

Example malicious entries previously observed associated with CHOSEN BRICK:

- Value name: **SMQDService**
  - Value data: **C: \ ProgramData \ SMQDServicePackages \ … \ smdqservice.exe**
- Value name: **winappx**
  - Value data: **C: \ Users \ All Users \ MicrosoftDistribution \ sysmain \ winappx.exe**

These filenames should **not be treated as exclusive indicators**, as the malware may change names, directories, or value names.

Check suspicious network communications

As CHOSEN BRICK interacts with numerous **legitimate** web services, it is likely to show up in corporate logging through DNS and web proxy services. Connections to these services, **where not expected** as part of normal business may indicate the presence of CHOSEN BRICK. The following domains appearing in logging unexpectedly should be investigated further:

- api[.]telegram[.]org
- backblazeb2[.]com
- vultrobjects[.]com
- storjshare[.]io
- iproyal[.]com
- lightningproxies[.]net

Mitigations

The best defence is for the user/victim to be more aware of social engineering through training. However, the following technical mitigations can help to prevent compromise where users manage their own devices:

1. Follow NCSC advice on staying safe online (e.g. don't install software sent via attachments or links and always use the direct, legitimate software download site or device app store).

2. Keep your devices up-to-date, ideally through automatic updates. This applies to all software, such as the operating system and all applications.
3. Use antivirus software and ensure it is enabled and always up-to-date.
4. Do not disable or ignore smart screen warnings on file downloads.

These additional mitigations can be enabled by network admins:

1. Enable phishing-resistant MFA.
2. Ensure devices are managed with appropriate controls enabled such as application allowlisting and antivirus.
3. Ensure you are using the email scanning and security functionality provided by your email provider.
4. Deploy endpoint and network monitoring.
5. Conduct a search for the IoCs included in this report across collected logs.

Contact

United Kingdom

Please report significant cyber security incidents to report.ncsc.gov.uk (monitored 24/7)

United States

Federal Bureau of Investigation If you or someone you know has fallen victim to this campaign, file a complaint with the FBI Internet Crime Complaint Center at www.ic3.gov

Netherlands

Any individual suspecting or confirming a compromise should contact the General Intelligence Security Service (https://www.aivd.nl) or local law enforcement authorities.

MITRE ATT&CK®

This report has been compiled with respect to the MITRE ATT&CK® framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

Tactic	ID	Technique	Procedure
Reconnaissance	T1589	Gather Victim Identity Information	Actor researches target to appear credible in social engineering
Initial Access	T1566.003	Phishing: Spear-phishing via Service	Actor social engineers target via social media, primarily Telegram
Execution	T1204.002	User Execution: Malicious File	Actor persuades target to open malicious file disguised as legitimate document/program
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	CHOSEN BRICK malware survives reboot using registry key “HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Run”
Defence Evasion	T1480.002	Execution Guardrails: Mutual Exclusion	CHOSEN BRICK malware registers mutexes, most commonly “ytyjyujyu” or “noi672pp434awkc12f”
Defence Evasion	T1685	Disable or Modify Tools	CHOSEN BRICK can add exclusions to Windows Defender antivirus to evade detection
Discovery	T1057	Process Discovery	CHOSEN BRICK can enumerate running processes

Disclaimer

This report draws on information derived from NCSC and industry sources. Any NCSC findings and recommendations made have not been provided with the intention of avoiding all risks and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.

All material is UK Crown Copyright ©

PUBLISHED

15 September 2026

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector

NEWS TYPE

Alert