D

Dyreza (Dyre) Banking Trojan: Credential Theft and Incident Response

Dyreza, also called Dyre, is Windows banking malware that intercepts browser sessions and steals credentials. Learn how it spread, what an alert means, and how to respond safely.

PUBLISHER
Gridinsoft Support

UPDATED
Aug 19, 2026

READ TIME
5 min

CONTENTS

In this guide

Dyreza, also called Dyre, is a Windows banking Trojan designed to steal credentials and interfere with online banking sessions. It became prominent in phishing campaigns during 2014 and 2015. Security products may use names such as Dyre, Dyreza, Dyzap, or family-specific signatures for related samples.

Dyreza is mainly a historical malware family, but a detection still matters. It can mean an old infected backup, a dormant file, a sample in an analyst collection, or code with behavior associated with the family. Do not assume that an old campaign name makes the affected computer safe.

01 What Dyreza does

- Targets credentials and data entered into banking and other high-value websites.
- Hooks or manipulates browser processes to observe sessions after a secure connection reaches the endpoint.
- Uses web injects or altered page content to request additional information.
- Communicates with command-and-control infrastructure over web protocols.
- Establishes persistence, including registration as a Windows service in documented variants.
- Can download configuration, modules, or additional malware.

HTTPS protects data between the browser and the website. It cannot protect information from malware already running inside the endpoint or browser session. A genuine padlock icon therefore does not rule out banking malware on the computer.

02 How Dyreza infections occurred

Documented campaigns used phishing email with attachments or links. The first file was often a downloader rather than the banking Trojan itself. Opening the lure allowed the downloader to retrieve Dyreza, start it, and establish persistence.

Stage	Typical activity	Evidence to preserve

Delivery	Phishing message, archive, document, or link	Original email, headers, attachment, URL, and delivery time
Execution	User opens content and a downloader starts	Process tree, command line, document history, and security alert
Installation	Payload is written and persistence is created	File path, hash, service, registry changes, and timestamps
Banking theft	Browser sessions and entered information are monitored or modified	Browser process activity, network logs, affected accounts, and transaction times
Command and control	Malware receives configuration or sends stolen data	DNS, proxy, firewall, and endpoint network telemetry

03 Possible warning signs

- A security product detects Dyre, Dyreza, Dyzap, Battdil, or a related downloader.
- An unexpected attachment or document launched a script, system utility, or executable.
- Online banking pages request unusual verification data or display unfamiliar fields.
- A browser process makes unexplained connections or loads a library from a user-writable folder.
- A new service, startup item, or scheduled task appears without a known installer.
- Fraudulent transactions or login alerts occur despite use of the correct bank website.

These signs are not sufficient to identify the family alone. Modern banking Trojans and infostealers can cause similar symptoms. Respond to the observed credential and financial risk even if the exact family name is uncertain.

04 What to do when Dyreza is detected

1. **Disconnect the affected computer.** Remove wired, wireless, VPN, and remote-access connections. Do not use it for banking or password changes.

2. **Preserve the alert context.** Record the detection name, file path, hash, time, user, parent process, and action taken by the security tool.
3. **Contact the financial institution from a clean device.** Explain that endpoint banking malware may have accessed the session. Review transactions, payees, account recovery details, and active devices.
4. **Change exposed credentials.** Start with email and banking accounts, then any password reused or entered on the infected system. Revoke sessions and replace compromised MFA methods.
5. **Run a full security scan.** Remove the detected file, downloader, persistence, and any additional payloads. Scan other devices that received the same message.
6. **Decide whether to rebuild.** A trusted Windows reinstall is appropriate when administrator access, browser injection, multiple payloads, or uncertain persistence prevents confidence in cleanup.
7. **Monitor after recovery.** Watch financial statements, email rules, account changes, identity alerts, and endpoint telemetry.

05 What if the file was only quarantined?

Quarantine prevents the detected object from running, but the incident scope depends on whether it executed. Check the original location, creation time, process history, email or download source, and whether related persistence or network activity exists.

If the file never executed, delete the lure and investigate how it arrived. If execution is possible, treat credentials and sessions used on that computer as exposed until the investigation shows otherwise.

06 Why a Dyreza detection may return

- A downloader, service, task, or startup item recreates the file.
- The same phishing attachment remains in mail, Downloads, or a synchronized folder.
- A backup or archive contains the old sample and is rescanned.

- Another device or shared folder restores the payload.
- The original remediation removed the banking Trojan but not the first-stage malware.

Use the detection path to guide the investigation. A file in an email cache calls for message removal; a file recreated under a system folder calls for persistence and parent-process analysis.

07 How to reduce banking-Trojan risk

- Block executable and script content from untrusted email where business needs allow.
- Keep Windows, browsers, document readers, and security software updated.
- Use application control and restrict script interpreters for users who do not need them.
- Require phishing-resistant MFA for email, financial, and administrative accounts.
- Verify unexpected payment documents or account notices through a separate channel.
- Use transaction alerts and bank controls such as payee approval or transfer limits.
- Separate everyday browsing from privileged financial administration in organizations.

08 Frequently asked questions

Are Dyre and Dyreza the same malware?

They are names used for the same banking-Trojan family. Vendors may also use related detection aliases or names for individual components.

Can Dyreza steal data from an HTTPS website?

Yes. HTTPS secures the network connection, but malware on the endpoint can capture or modify information before encryption or after decryption.

Is Dyreza still active?

The best-known campaigns are historical. A current alert can still identify an old artifact or related sample, and the possibility that it executed requires normal incident response rather than dismissal.

09 References

- MITRE ATT&CK: Dyre (S0024)
- CISA: Phishing campaign linked with Dyre banking malware
- Cisco Talos: Dyre/Dyreza technical analysis
- Malwarebytes: A technical look at Dyreza