Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:19:31 UTC

Tool: Dyre

Names	Dyre Dyreza Dyzap Dyranges
Category	Malware
Type	Banking trojan, Info stealer, Backdoor
Description	(SecureWorks) In early June 2014, the Dell SecureWorks Counter Threat Unit (CTU) research team discovered the banking trojan, which was being distributed by Cutwail botnet spam emails that included links to either Dropbox or file storage services. The threat actors later shifted to distribution via the Upatre downloader trojan. Dyre is also kn Dyreza, Dyzap, and Dyranges by the antivirus industry. Dyre harvests credentials, primarily targeting online banking websites to perform Automated Clearing House (ACH wire fraud. The malware includes a modular architecture, man-in-the-browser functionality, and a backconnect serv allows threat actors to connect to a bank website through the victim's computer. The man-in-the-browser functional based on a unique combination of redirects to fake websites controlled by the threat actor ('web fakes') and a dynam inject system that allows the threat actors to manipulate a financial institution's website content. Similar to other ban trojans, Dyre hooks into the most popular web browsers to intercept traffic from a victim's system, stealing informa manipulating website content before it is rendered by the browser. Early Dyre versions were relatively primitive, sending command and control (C2) communications and stolen data unencrypted HTTP. Recent iterations of Dyre use SSL to encrypt all C2 communications, as well as a custom encry algorithm. Dyre also uses RSA cryptography to digitally sign configuration files and malware plugins to prevent tan
Information	<https://www.secureworks.com/research/dyre-banking-trojan> <https://www.blueliv.com/downloads/documentation/reports/Network_insights_of_Dyre_and_Dridex_Trojan_bank <https://blog.malwarebytes.com/threat-analysis/2015/11/a-technical-look-at-dyreza/> <https://www.forbes.com/sites/thomasbrewster/2017/05/04/dyre-hackers-stealing-millions-from-american-coporate <https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0024/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.dyre>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag;Dyre>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool Dyre

Changed	Name	Country	Observed

APT groups

	Wizard Spider, Gold Blackburn		2014-May 2025	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=1b27f8b4-dddf-4d58-b033-3772234bdd47