Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:52:37 UTC

Tool: Backswap

Names	Backswap
Category	Malware
Type	Banking trojan, Credential stealer
Description	(CERT.PL) Backswap is a banker, which we first observed around March 2018. It's a variant of old, well-known malware Tinba (which stands for "tiny banker"). As the name suggests, it's main characteristic is small size (very often in the 10-50kB range). Backswap carries out multiple harmful activities. Big ones are: injecting Webinjects and stealing credentials. Supported browsers involve Internet Explorer, Mozilla Firefox, Google Chrome. Some variants also swap the contents of the clipboard when bank/cryptocurrency account number is found.
Information	<https://www.cert.pl/en/news/single/backswap-malware-analysis/> <https://research.checkpoint.com/2018/the-evolution-of-backswap/> <https://securityintelligence.com/backswap-malware-now-targets-six-banks-in-spain/> <https://www.f5.com/labs/articles/threat-intelligence/backswap-defrauds-online-banking-customers-using-hidden-input-fi> <https://www.cyberbit.com/blog/endpoint-security/backswap-banker-malware-hides-inside-replicas-of-legitimate-programs/> <https://www.welivesecurity.com/2018/05/25/backswap-malware-empty-bank-accounts/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.backswap>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Backswap>

Last change to this tool card: 24 May 2020

Download this tool card in JSON format

All groups using tool Backswap

Changed	Name	Country	Observed

Unknown groups

	[Interesting malware not linked to an actor yet]			

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=918148af-92e2-42dc-b5bd-eb700a11ec39