Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:05:09 UTC

Tool: URLZone

Names	URLZone Bebloh Shiotob
Category	Malware
Type	Banking trojan, Info stealer, Credential stealer
Description	(FireEye) URLZone is a banking trojan. It downloads a configuration file that contains information on targeted financial institutions, and uses web injection techniques to steal a user's banking credentials.
Information	<https://www.fireeye.com/blog/threat-research/2016/01/urlzone_zones_inon.html> <https://www.gdatasoftware.com/blog/2013/12/23978-bebloh-a-well-known-banking-trojan-with-noteworthy-innovations> <https://www.johannesbader.ch/2015/01/the-dga-of-shiotob/> <https://www.proofpoint.com/us/threat-insight/post/Vawtrak-UrlZone-Banking-Trojans-Target-Japan> <https://www.arbornetworks.com/blog/asert/an-update-on-the-urlzone-banker/> <https://www.cybereason.com/blog/new-ursnif-variant-targets-japan-packed-with-new-features> <https://www.crowdstrike.com/blog/cutwail-spam-campaign-uses-steganography-to-distribute-urlzone/> <https://www.virusbulletin.com/virusbulletin/2012/09/urlzone-reloaded-new-evolution/> <http://blog.inquest.net/blog/2019/03/09/Analyzing-Sophisticated-PowerShell-Targeting-Japan/> <https://krebsonsecurity.com/2011/07/trojan-tricks-victims-into-transfering-funds/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.urlzone>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:urlzone>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool URLZone

Changed	Name	Country	Observed	
Other groups				
	Bamboo Spider, TA544	[Unknown]	2016-Apr 2022	

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

↑
