Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:47:19 UTC

Tool: Chthonic

Names	Chthonic AndroKINS
Category	Malware
Type	Banking trojan
Description	(Kaspersky) In the fall of 2014, we discovered a new banking Trojan, which caught our attention for two reasons: • First, it is interesting from the technical viewpoint, because it uses a new technique for loading modules. • Second, an analysis of its configuration files has shown that the malware targets a large number of online-banking systems: over 150 different banks and 20 payment systems in 15 countries. Banks in the UK, Spain, the US, Russia, Japan and Italy make up the majority of its potential targets. Kaspersky Lab products detect the new banking malware as Trojan-Banker.Win32.Chthonic. The Trojan is apparently an evolution of ZeusVM, although it has undergone a number of significant changes. Chthonic uses the same encryptor as Andromeda bots, the same encryption scheme as Zeus AES and Zeus V2 Trojans, and a virtual machine similar to that used in ZeusVM and KINS malware.
Information	<https://securelist.com/chthonic-a-new-modification-of-zeus/68176/> <https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan> <https://www.s21sec.com/en/blog/2017/07/androkins/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.chthonic>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:chthonic>

Last change to this tool card: 24 May 2020

Download this tool card in JSON format

All groups using tool Chthonic

Changed	Name	Country	Observed	
Other groups				
	Bamboo Spider, TA544	[Unknown]	2016-Apr 2022	
	TA516	[Unknown]	2016-Feb 2020	

2 groups listed (0 APT, 2 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=56684ac2-715b-418e-a3e5-34af3ee7b408