Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:49:34 UTC

Tool: Gozi

Names	Gozi CRM Gozi CRM Papras Ursnif Snifula
Category	Malware
Type	Banking trojan, Credential stealer
Description	(SecureWorks) A single attack by a single variant compromises more than 5200 hosts and 10,000 user accounts on hundreds of sites. • Steals SSL data using advanced Winsock2 functionality • State-of-the-art, modularized trojan code • Spread through IE browser exploits • Undetected for weeks, months by many AV vendors • Customized server/database code to collect sensitive data • Customer interface for on-line purchases of stolen data • Accounts compromised by stealing data primarily from infected home PCs • Accounts at top financial, retail, health care, and government services affected • Data's black market value at least $2 million
Information	<https://www.secureworks.com/research/gozi> <https://blog.gdatasoftware.com/2016/11/29325-analysis-ursnif-spying-on-your-data-since-2007> <http://researchcenter.paloaltonetworks.com/2017/02/unit42-banking-trojans-ursnif-global-distribution-networks-identified/> <https://lokalhost.pl/gozi_tree.txt> <https://blog.avast.com/ursnif-victim-data> <https://securityintelligence.com/posts/ursnif-cerberus-android-malware-bank-transfers-italy/> <https://www.mandiant.com/resources/blog/rm3-ldr4-ursnif-banking-fraud>

	<https://securityintelligence.com/posts/gozi-strikes-again-targeting-banks-cryptocurrency-and-more/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:gozi>

Last change to this tool card: 06 September 2023

Download this tool card in JSON format

All groups using tool Gozi

Changed	Name	Country	Observed	
Other groups				
	TA551, Shathak		2016-Jan 2021	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

2 groups listed (0 APT, 1 other, 1 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f8740da3-1d35-498a-a026-74ce0c034f6d