Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:08:10 UTC

Tool: BernhardPOS

Names	BernhardPOS
Category	Malware
Type	POS malware, Credential stealer
Description	(securitykitten) What makes BernhardPOS stand out is the use of code that continues to evade AV detection. Between manually resolving imports when they are needed and inserting junk code between legit operations, this malware stays successfully hidden. It manually encodes the strings that it needs to in order to evade a simple string based rule. And it doesn't heavily pack or encrypt itself in a way that would set off high entropy rules. In most network scenarios, DNS is a port left wide open due to machines needing to communicate with one another and the larger Internet. Leveraging DNS allows the malware authors to not worry about being blocked by a firewall or hindered by network restrictions.
Information	<https://securitykitten.github.io/2015/07/14/bernhardpos.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.bernhardpos>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:BernhardPOS>

Last change to this tool card: 24 May 2020

Download this tool card in JSON format

All groups using tool BernhardPOS

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

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