Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:12:06 UTC

Tool: Hisoka

Names	Hisoka
Category	Malware
Type	Backdoor, Downloader
Description	(Palo Alto) We analyzed dozens of samples during this analysis, which resulted in the identification of two separate campaigns — one in mid-to-late 2018 using Sakabota and the other in mid-2019 using Hisoka. Our analysis of the two campaigns revealed that Sakabota is the predecessor to Hisoka, which was first observed in May 2019. During our analysis, we identified two different versions of Hisoka, specifically v0.8 and v0.9, both installed onto the network of two Kuwait organizations. Both versions contain command sets that allow the actor to control a compromised system. In both versions, the actor can communicate via a command and control (C2) channel that uses either HTTP or DNS tunneling. However, v0.9 also added the ability for an email-based C2 channel as well. The email-based C2 communications capability added to Hisoka v0.9 relies on Exchange Web Services (EWS) to use a legitimate account on an Exchange server in order to allow the actor to communicate with Hisoka. The malware attempts to log into an Exchange server using supplied credentials and uses EWS to send and receive emails in order to establish communications between the target and the actor. However, the communications channel does not actually send and receive emails like other email-based C2 channels we have seen in the past. Instead, the channel relies on creating email drafts that the Hisoka malware and the actor will process in order to exchange data back and forth. By using email drafts as well as the same legitimate Exchange account to communicate, no emails will be detected outbound or received inbound. Within two hours of gaining access to the system through Hisoka, the actor deployed two additional tools named Gon and EYE, whose names were based on the filenames Gon.sys and EYE.exe.
Information	<https://unit42.paloaltonetworks.com/xhunt-campaign-attacks-on-kuwait-shipping-and-transportation-organizations/>

Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.hisoka>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Hisoka

Changed	Name	Country	Observed	
APT groups				
	xHunt		2018-Aug 2019	

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