Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:14:41 UTC

APT group: xHunt

Names	xHunt *(Palo Alto)* SectorD01 *(ThreatRecon)* Hive0081 *(IBM)* Cobalt Katana *(SecureWorks)* Hunter Serpens *(Palo Alto)*
Country	Iran
Motivation	Information theft and espionage
First seen	2018
Description	(Palo Alto) Between May and June 2019, Unit 42 observed previously unknown tools used in the targeting of transportation and shipping organizations based in Kuwait. The first known attack in this campaign targeted a Kuwait transportation and shipping company in which the actors installed a backdoor tool named Hisoka. Several custom tools were later downloaded to the system in order to carry out post-exploitation activities. All of these tools appear to have been created by the same developer. We were able to collect several variations of these tools including one dating back to July 2018. The developer of the collected tools used character names from the anime series Hunter x Hunter, which is the basis for the campaign name “xHunt.” The names of the tools collected include backdoor tools Sakabota, Hisoka, Netero and Killua. These tools not only use HTTP for their command and control (C2) channels, but certain variants of these tools use DNS tunneling or emails to communicate with their C2 as well. While DNS tunneling as a C2 channel is fairly common, the specific method in which this group used email to facilitate C2 communications has not been observed by Unit 42 in quite some time. This method uses Exchange Web Services (EWS) and stolen credentials to create email “drafts” to communicate between the actor and the tool. In addition to the aforementioned backdoor tools, we also observed tools referred to as Gon and EYE, which provide the backdoor access and the ability to carry out post-exploitation activities.

Observed	Sectors: Shipping and Logistics. Countries: Kuwait.	
Tools used	BumbleBee, CASHY200, Gon, EYE, Hisoka, Killua, Netero, Sakabota, Snugy, TriFive.	
Operations performed	May 2018	On May 1 and June 3, 2018, we first saw executables that installed and executed CASHY200 PowerShell scripts <https://unit42.paloaltonetworks.com/more-xhunt-new-powershell-backdoor-blocked-through-dns-tunnel-detection/>
	Aug 2019	Newly Discovered Backdoors Using Deleted Email Drafts and DNS Tunneling for Command and Control <https://unit42.paloaltonetworks.com/xhunt-campaign-backdoors/> <https://unit42.paloaltonetworks.com/bumblebee-webshell-xhunt-campaign/>
Information	<https://unit42.paloaltonetworks.com/xhunt-campaign-attacks-on-kuwait-shipping-and-transportation-organizations/>	
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=hunter-serpens>	

Last change to this card: 10 March 2024

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=3a8ec920-4dfd-4a06-81e7-7be8ee639b73