Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:45:06 UTC

APT group: Orangeworm

Names	Orangeworm *(Symantec)* G0071 *(MITRE)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2015
Description	(Symantec) Symantec has identified a previously unknown group called Orangeworm that has been observed installing a custom backdoor called Trojan.Kwampirs within large international corporations that operate within the healthcare sector in the United States, Europe, and Asia. First identified in January 2015, Orangeworm has also conducted targeted attacks against organizations in related industries as part of a larger supply-chain attack in order to reach their intended victims. Known victims include healthcare providers, pharmaceuticals, IT solution providers for healthcare and equipment manufacturers that serve the healthcare industry, likely for the purpose of corporate espionage. Based on the list of known victims, Orangeworm does not select its targets randomly or conduct opportunistic hacking. Rather, the group appears to choose its targets carefully and deliberately, conducting a good amount of planning before launching an attack. According to Symantec telemetry, almost 40 percent of Orangeworm's confirmed victim organizations operate within the healthcare industry. The Kwampirs malware was found on machines which had software installed for the use and control of high-tech imaging devices such as X-Ray and MRI machines. Additionally, Orangeworm was observed to have an interest in machines used to assist patients in completing consent forms for required procedures. The exact motives of the group are unclear.

	(Cylera Labs) At Cylera Labs we assess with medium-high confidence that Shamoon (OilRig, APT 34, Helix Kitten, Chrysene) and Kwapirs are the same group or really close collaborators, sharing updates, techniques and code over the course of multiple years.	
Observed	Sectors: Food and Agriculture, Healthcare, IT, Manufacturing, Shipping and Logistics. Countries: Belgium, Brazil, Canada, Chile, China, France, Germany, Hong Kong, Hungary, India, Malaysia, Netherlands, Norway, Philippines, Poland, Saudi Arabia, Spain, Sweden, Switzerland, Turkey, UK, USA.	
Tools used	Kwampirs, Living off the Land.	
Operations performed	Jan 2020	The FBI has issued an alert on Monday about state-sponsored hackers using the Kwampirs malware to attack supply chain companies and other industry sectors as part of a global hacking campaign. <https://www.zdnet.com/article/fbi-re-sends-alert-about-supply-chain-attacks-for-the-third-time-in-three-months/>
Information	<https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia> <https://resources.cylera.com/new-evidence-linking-kwampirs-malware-to-shamoon-apts>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0071/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
