Russian state unit targets Ukrainian software development entity with GoMet backdoor

21st July 2022

Orpheus vulnerability severity score: 59

A Russian nation-state unit has targeted a Ukrainian software development company with a modified version of the open-source GoMet backdoor.

The GoMet backdoor, written in the Go programming language, has been available on GitHub since 2019. It supports single command execution, file upload, file download, and deploying shells. Additionally, it can execute daisy chains, whereby the operator gains access to a network or machine and uses information from the target to access multiple networks and machines. This feature enables persistent access and allows the operator to interact with hosts, which would otherwise be isolated from the Internet.

The victim provides software to multiple government entities in Ukraine, therefore the perpetrators may have intended to gain access to the victim's infrastructure to launch a supply-chain compromise. We have previously reported that the Russian espionage unit APT29 (also known as Nobelium) targeted technology service providers to access and compromise customers downstream of the initial victim.

Ukraine has been subject to multiple campaigns of Russian origin seeking to compromise targets across several sectors with backdoors, including the DarkCrystal remote access trojan, GrimPlant, GraphSteel, and Pteranodon.

This incident reaffirms that while the frequency of destructive Russian state-sponsored operations targeting Ukraine has decreased over the past few months, it is still defending itself against resolute and well-funded adversaries that intend to cause widespread disruption to its critical infrastructure. Russian state units will likely continue to develop new methods to gain persistent access to Ukrainian targets of strategic importance.

+44 (0)203 8232 999
info@secrutiny.com
www.secrutiny.com

Threat Subcategory	Russia
Sectors	Technology
Objective	Infrastructure enumeration/compromise
Countries & Target	Russia, Ukraine
Malware & Tools	GoMet
Source	https://blog.talosintelligence.com/2022/07/attackers-target-ukraine-using-gomet.html