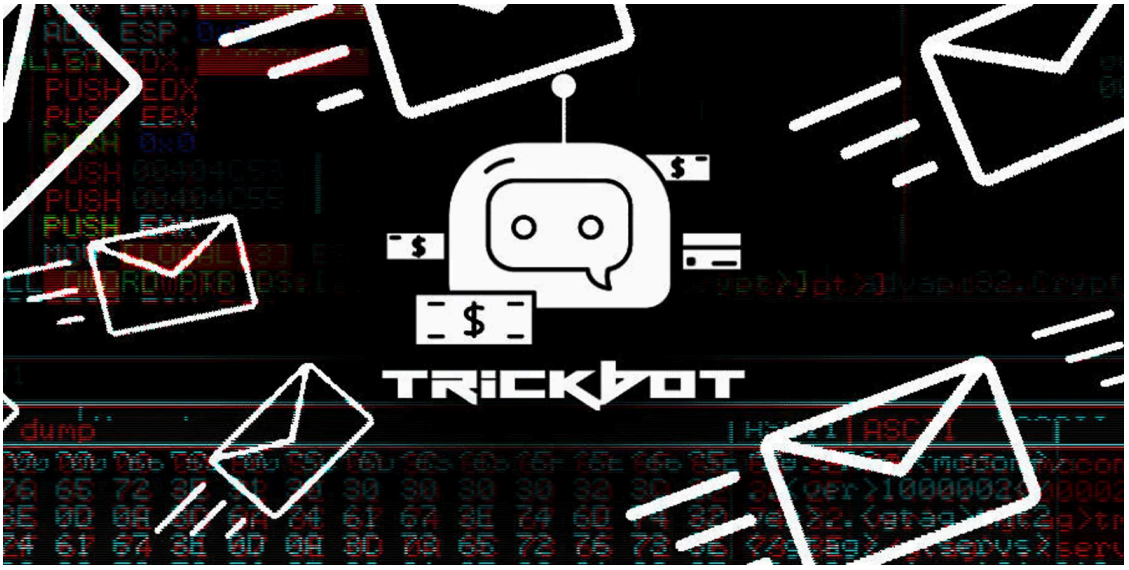
TrickBot's BazarBackdoor malware is now coded in Nim to evade antivirus

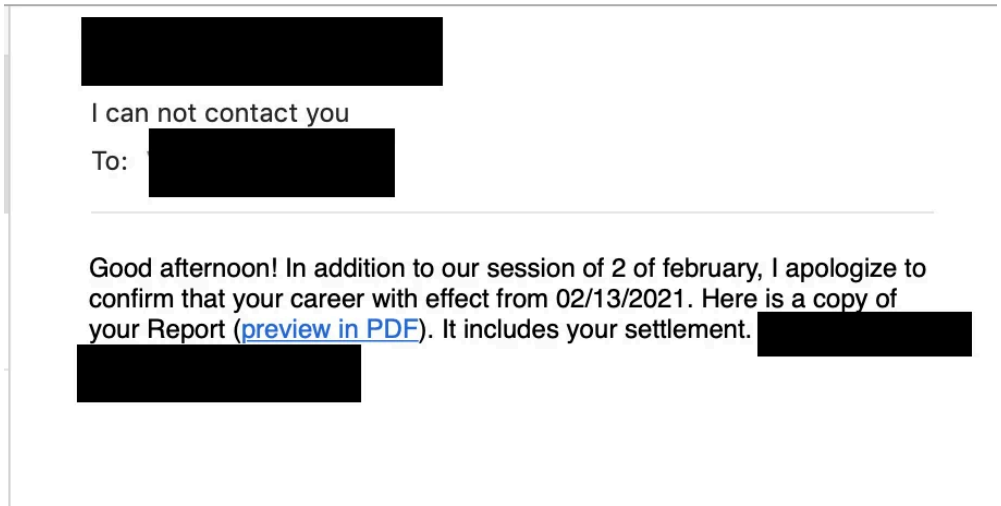
By Lawrence Abrams

Published: 2021-02-11 · Archived: 2026-04-05 14:16:34 UTC



TrickBot's stealthy BazarBackdoor malware has been rewritten in the Nim programming language, likely to evade detection by security software.

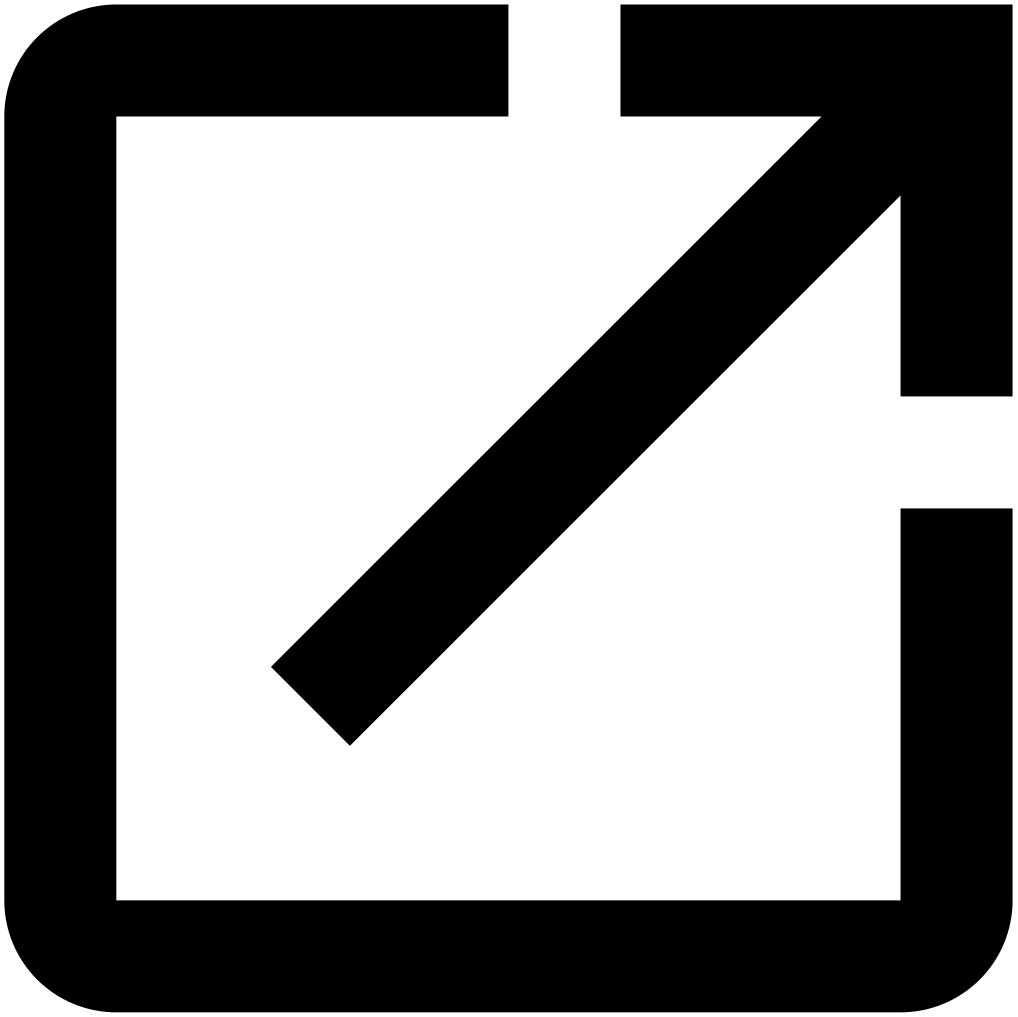
The TrickBot cybercrime gang has been increasingly distributing their newer and stealthier BazarBackdoor malware through spam campaigns. Once a computer becomes infected, BazarBackdoor is used to provide the threat actors remote access to the computer to spread laterally throughout a network.



BazarBackdoor phishing email

Last week, both cybersecurity firm Intezer and Advanced Intel's Vitali Kremez analyzed a new sample of BazarBackdoor and discovered that the TrickBot gang ported it to the Nim programming language.


DIE LINKE.
0:00



According to the programming language's website, Nim takes its inspiration from Python, Ada, and Modula and can generate executables supported on Windows, macOS, and Linux.

"Nim is one of the very few *programmable* statically typed languages, and combines the speed and memory efficiency of C, an expressive syntax, memory safety and multiple target languages." states the Nim website.

As it is rare to find malware developed using Nim, Kremez believes that the TrickBot gang ported BazarBackdoor to Nim to bypass detection by antivirus software.

"The backdoor component that is capable of command execution is written in NIM programming language to evade anti-virus detection. The crime group likely chose to pursue the lightweight malware development in Nim to frustrate anti-virus and detection mechanism focused on traditional binaries compiled in C/C++ style languages."

"Not too long ago, Golang has become another preferred language of choice for some malware families including RobbinHood ransomware majorly due to the fact that many anti-virus products fail to process and characterize unconventional binaries as malware due to unique section and binary content introduced by the Nim and similar exotic languages," Advanced Intel CEO Vitali Kremez told BleepingComputer in a conversation.

Other malware developed in Nim is a ransomware family called XCry [VirusTotal] discovered by MalwareHunterTeam in 2019.

More recently, the Nim-coded DeroHE ransomware [VirusTotal] was used in an attack against IObit forum users.

Nim is not the only uncommon language recently used to create malware. Last month, Kremez found that the new Vovalex ransomware was written in the D programming language.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
