What does Go-written malware look like? Here's a sample under the microscope

By Jeff Burt

Published: 2022-03-22 · Archived: 2026-04-05 16:52:36 UTC

The folks at Deep Instinct say they have studied a Go-written variant of the malware used by the Arid Viper cyber-crime ring.

Deep Instinct, founded in 2015, says it uses deep learning to detect and block malware. While training a deep-learning model that's focused on identifying software nasties written in Go, the researchers uncovered an executable file built using the programming language, submitted it to the VirusTotal website, and found only six security vendors had the binary flagged as malicious.

Further investigation uncovered two similar Go-written binaries. From these programs, we're told, it became clear the team were looking at a variant of Micropsia. This malware was identified in 2017 and is used exclusively by Arid Viper, an advanced persistent threat (APT) group believed to be based in Gaza and known as APT-C-23. Deep Instinct named the Go-written malware Arid Gopher.

"This new variant is still being developed; all the three files share a common baseline, but each file contains unique code which is not present in the other files," Deep Instinct researchers Simon Kenin and Asaf Gilboa wrote in an analysis this Monday. "Beside the main implant, our investigation revealed a 'helper' malware, also written in Go, and a second-stage malware which was downloaded from the C2 [command-and-control] server."

Essentially, Arid Gopher has the same functionality of Arid Viper; it is simply written in the Go language.

"This is also how we related it to Arid Viper," Moshe Hayun, Deep Instinct's threat intelligence team leader, told *The Register*. "We used code similarities and functionality similarities. This is how we found out it's the same actor, using the decompiler, reverse engineering, and looking into the functionalities and how it does things."

Kenin told *The Register* that writing the code in Go was likely a way to bypass detection. It's not unusual to see threat groups shift the programming language they use to keep malware under the radar. In its 2022 Cyber Threat Landscape Report released in February, Deep Instinct said that in 2021 it saw a shift by gangs away from older languages like C and C++ to newer ones, including Python and Go, which are easy to learn.

Antivirus engines may be unfamiliar with the structure or identities of executables produced from these newer languages; a binary built from C++ may be in a malware database, but the binary of a rewrite in Go may not be, buying its creators some extra time to avoid detection. It could also be cyber-crooks are just keeping up with software development trends, tools, and libraries.

In Arid Viper's case, its masterminds have used a range of programming languages, jumping from Pascal and Delphi to C++, Python, and now Go. What hasn't changed is how the malware works or what it is designed to do.

"APTs, their sole purpose is to infiltrate important assets," Hayun said. "I don't know if I have seen an APT transposing from so many languages, like Delphi [and] Pascal, but Go malware is kind of a trend now because it's a new language, it has a lot of open-source libraries, a lot of libraries like helper functions to collect information from the victim's computers and stuff like that. I don't know how unique it is. APTs do that. Their models are out there in several languages. I don't recall anyone APT using these exact languages or transposing it to Go."

According to Deep Instinct, Arid Viper's malware targets computers running Microsoft Windows, and has been used primarily in the Middle East, with a specific focus on Palestinian targets. It has been linked in the past to Hamas, according to the researchers. There also is an Android strain apparently used against Israeli targets, and last year Facebook-owner Meta issued a report [PDF] that identified an iOS nasty developed by Arid Viper.

- Microsoft investigates after Lapsus$ gang brags of Bing, Cortana code heist
- Western Digital tells EdgeRover users to patch app again
- AvosLocker group is targeting US critical infrastructure, FBI says
- Take this $715,000 and find security gaps in quantum computers, says NSF

Deep Instinct outlined the Arid Gopher variants it uncovered. Arid Gopher V1 is written in Go 1.16.5gs and includes code from libraries available from GitHub, which the researchers noted "saves the author time by not needing to write some features from scratch. It also adds some degree of legitimacy because those libraries are not malicious, but the malware author abuses the libraries' capabilities for malicious purposes."

There are two versions of the Arid Gopher V2 variant that have been used since the beginning of the year. Both samples were written in Go 1.17.4 and use some of the public libraries from GitHub that are in V1. A key difference between the two is the content of the benign documents they save on a victim's desktop, the team wrote. The variants are emailed to targets in .xz RAR archives, and unpack with a long filename to hopefully push their .exe extension out of sight. When successfully run, they infect the host Windows PC, open a backdoor to a command-and-control server to receive further instructions, and drop a decoy document on the desktop and display it so that the victim thinks they've simply saved and opened an attached Word file and not malware.

The variants also continue Arid Viper's use of names of characters in popular TV shows in their domain names. In V1, the name Grace Fraser is used in a domain name. Grace Fraser is a character in the HBO series The Undoing. In V2, a name used is Pam Beesly, a character from the sitcom The Office.

Gilboa and Kenin claim deep learning gives them an edge over rival cybersecurity vendors in finding malicious code. The researchers wrote that some competitors rely on manually tuned heuristics, or manually selected features that are fed into classical machine-learning models, to determine if a file is malicious or legitimate. Other methods include running programs in a sandbox to get more information.

Deep Instinct instead trains models to learn as they go.

"Researchers are manually going over samples and then are updating their signature mechanism," Hayun said. "We do it a bit differently. We take huge amounts of data, so there is a really high probability that our deep learning models already saw something similar.

"They say, 'I saw something similar. I know that this and this and this will increase the probability of something being malicious,' so the next time something a bit similar comes into the model, it will say, 'I saw something

similar like this. I will give it the highest quality to be this as malicious.'" ®
