

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

 [theregister.com/2022/03/22/arid-gopher-malware-deep-instinct/](https://www.theregister.com/2022/03/22/arid-gopher-malware-deep-instinct/)

Jeff Burt



Security

Arid Gopher sticks its head out from its burrow

[Jeff Burt](#) Tue 22 Mar 2022 // 03:53 UTC

6 

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.

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.'" ®

Other stories you might like

- [Big Tech loves talking up privacy – while trying to kill privacy legislation](#)

[Study claims Amazon, Apple, Google, Meta, Microsoft work to derail data rules](#)

[Thomas Claburn in San Francisco](#) Fri 27 May 2022 // 21:48 UTC 

Amazon, Apple, Google, Meta, and Microsoft often support privacy in public statements, but behind the scenes they've been working through some common organizations to weaken or kill privacy legislation in US states.

That's according to [a report](#) this week from news non-profit The Markup, which said the corporations hire lobbyists from the same few groups and law firms to defang or drown state privacy bills.

The report examined 31 states when state legislatures were considering privacy legislation and identified 445 lobbyists and lobbying firms working on behalf of Amazon, Apple, Google, Meta, and Microsoft, along with industry groups like TechNet and the State Privacy and Security Coalition.

[Continue reading](#)

- [SEC probes Musk for not properly disclosing Twitter stake](#)

[Meanwhile, social network's board rejects resignation of one its directors](#)

[Katyanna Quach](#) Fri 27 May 2022 // 21:26 UTC 

America's financial watchdog is investigating whether Elon Musk adequately disclosed his purchase of Twitter shares last month, just as his bid to take over the social media company hangs in the balance.

A letter [\[PDF\]](#) from the SEC addressed to the tech billionaire said he "[did] not appear" to have filed the proper form detailing his 9.2 percent [stake](#) in Twitter "required 10 days from the date of acquisition," and asked him to provide more information. Musk's shares made him one of Twitter's largest shareholders.

Musk quickly moved to try and buy the whole company outright in a deal initially worth over \$44 billion. Musk sold a chunk of his shares in Tesla worth \$8.4 billion and [bagged](#) another \$7.14 billion from investors to help finance the \$21 billion he [promised](#) to put forward for the deal. The remaining \$25.5 billion bill was secured via debt financing by Morgan Stanley, Bank of America, Barclays, and others. But the takeover is not going smoothly.

[Continue reading](#)

- [Cloud security unicorn cuts 20% of staff after raising \\$1.3b](#)

[Time to play blame bingo: Markets? Profits? Too much growth? Russia? Space aliens?](#)

[Jessica Lyons Hardcastle](#) Fri 27 May 2022 // 19:19 UTC 2 

Cloud security company Lacework has laid off 20 percent of its employees, just months after two record-breaking funding rounds pushed its valuation to \$8.3 billion.

A spokesperson wouldn't confirm the total number of employees affected, though told *The Register* that the "widely speculated number on Twitter is a significant overestimate."

The company, as of March, counted more than 1,000 employees, which would push the jobs lost above 200. And the widely reported number on Twitter is about 300 employees. The biz, based in Silicon Valley, was founded in 2015.

[Continue reading](#)

- [Talos names eight deadly sins in widely used industrial software](#)

[Entire swaths of gear relies on vulnerability-laden Open Automation Software \(OAS\)](#)

[Jeff Burt](#) Fri 27 May 2022 // 18:30 UTC 

A researcher at Cisco's Talos threat intelligence team found eight vulnerabilities in the Open Automation Software (OAS) platform that, if exploited, could enable a bad actor to access a device and run code on a targeted system.

The OAS platform is widely used by a range of industrial enterprises, essentially facilitating the transfer of data within an IT environment between hardware and software and playing a central role in organizations' industrial Internet of Things (IIoT) efforts. It touches a range of devices, including PLCs and OPCs and IoT devices, as well as custom applications and APIs, databases and edge systems.

Companies like Volvo, General Dynamics, JBT Aerotech and wind-turbine maker AES are among the users of the OAS platform.

[Continue reading](#)

- [Despite global uncertainty, \\$500m hit doesn't rattle Nvidia execs](#)

[CEO acknowledges impact of war, pandemic but says fundamentals 'are really good'](#)

[Dylan Martin](#) Fri 27 May 2022 // 16:08 UTC 1 

Nvidia is expecting a \$500 million hit to its global datacenter and consumer business in the second quarter due to COVID lockdowns in China and Russia's invasion of Ukraine. Despite those and other macroeconomic concerns, executives are still optimistic about future prospects.

"The full impact and duration of the war in Ukraine and COVID lockdowns in China is difficult to predict. However, the impact of our technology and our market opportunities remain unchanged," said Jensen Huang, Nvidia's CEO and co-founder, during the company's first-quarter earnings call.

Those two statements might sound a little contradictory, including to some investors, particularly following the [stock selloff](#) yesterday after concerns over Russia and China prompted Nvidia to issue lower-than-expected guidance for second-quarter revenue.

[Continue reading](#)

- [Another AI supercomputer from HPE: Champollion lands in France](#)

[That's the second in a week following similar system in Munich also aimed at researchers](#)

[Dan Robinson](#) Fri 27 May 2022 // 15:30 UTC 

HPE is lifting the lid on a new AI supercomputer – the second this week – aimed at building and training larger machine learning models to underpin research.


Based at HPE's Center of Excellence in Grenoble, France, the new supercomputer is to be named Champollion after the French scholar who made advances in deciphering Egyptian hieroglyphs in the 19th century. It was built in partnership with Nvidia using AMD-based Apollo computer nodes fitted with Nvidia's A100 GPUs.

Champollion brings together HPC and purpose-built AI technologies to train machine learning models at scale and unlock results faster, HPE said. HPE already provides HPC and AI resources from its Grenoble facilities for customers, and the broader research community to access, and said it plans to provide access to Champollion for scientists and engineers globally to accelerate testing of their AI models and research.

[Continue reading](#)

- [Workday nearly doubles losses as waves of deals pushed back](#)

[Figures disappoint analysts as SaaS HR and finance application vendor navigates economic uncertainty](#)

[Lindsay Clark](#) Fri 27 May 2022 // 14:30 UTC 7 

HR and finance application vendor Workday's CEO, Aneel Bhusri, confirmed deal wins expected for the three-month period ending April 30 were being pushed back until later in 2022.

The SaaS company boss was speaking as Workday recorded an operating loss of \$72.8 million in its first quarter [[PDF](#)] of fiscal '23, nearly double the \$38.3 million loss recorded for the same period a year earlier. Workday also saw revenue increase to \$1.43 billion in the period, up 22 percent year-on-year.

However, the company increased its revenue guidance for the full financial year. It said revenues would be between \$5.537 billion and \$5.557 billion, an increase of 22 percent on earlier estimates.

[Continue reading](#)

- [UK monopoly watchdog investigates Google's online advertising business](#)

[Another probe? Mountain View is starting to look like a pincushion at this rate](#)

[Richard Currie](#) Fri 27 May 2022 // 14:00 UTC 3 

The UK's Competition and Markets Authority is lining up yet another investigation into Google over its dominance of the digital advertising market.

This latest inquiry, [announced Thursday](#), is the second major UK antitrust investigation into Google this year alone. In March this year the UK, together with the European Union, said it wished to examine Google's "[Jedi Blue](#)" [agreement](#) with Meta to allegedly favor the former's Open Bidding ads platform.

The news also follows [proposals](#) last week by a bipartisan group of US lawmakers to create legislation that could force Alphabet's Google, Meta's Facebook, and Amazon to divest portions of their ad businesses.

[Continue reading](#)

- [Microsoft slows some hiring for Windows, Teams, and Office](#)

['Making sure the right resources are aligned to the right opportunity' ahead of next fiscal year](#)

[Richard Speed](#) Fri 27 May 2022 // 13:31 UTC 4 

Microsoft has hit the brakes on hiring in some key product areas as the company prepares for the next fiscal year and all that might bring.

According to reports in the [Bloomberg](#), the unit that develops Windows, Office, and Teams is affected and while headcount remains expected to grow, new hires in that division must first be approved by bosses.

During a talk this week at JP Morgan's Technology, Media and Communications Conference, Rajesh Jha, executive VP for the Office Product Group, noted that within three years he expected approximately two-thirds of CIOs to standardize on Microsoft Teams. 1.4 billion PCs were running Windows. He also remarked: "We have lots of room here to grow the seats with Office 365."

[Continue reading](#)

- [Recession fears only stoking enterprise tech spending for Dell, others](#)

[Staving off entropy with digital transformation, hybrid office, and automation projects](#)

[Paul Kunert](#) Fri 27 May 2022 // 13:00 UTC 

Enterprises are still kitting out their workforce with the latest computers and refreshing their datacenter hardware despite a growing number of "uncertainties" in the world.

This is according to hardware tech bellwethers including Dell, which turned over \$26.1 billion in sales for its [Q1 of fiscal 2023 ended 29 April](#), a year-on-year increase of 16 percent.

"We are seeing a shift in spend from consumer and PCs to datacenter infrastructure," said Jeff Clarke, vice-chairman and co-chief operating officer. "IT demand is currently healthy," he added.

[Continue reading](#)

- [GitHub saved plaintext passwords of npm users in log files, post mortem reveals](#)

[Unrelated to the OAuth token attack, but still troubling as org reveals details of around 100,000 users were grabbed by the baddies](#)

Richard Speed Fri 27 May 2022 // 12:15 UTC 7 

GitHub has revealed it stored a "number of plaintext user credentials for the npm registry" in internal logs following the integration of the JavaScript package registry into GitHub's logging systems.

The information came to light when the company [today published](#) the results of its investigation into April's unrelated OAuth token theft attack, where it described how an attacker grabbed data including the details of approximately 100,000 npm users.

The code shack went on to assure users that the relevant log files had not been leaked in any data breach; that it had improved the log cleanup; and that it removed the logs in question "prior to the attack on npm."

[Continue reading](#)