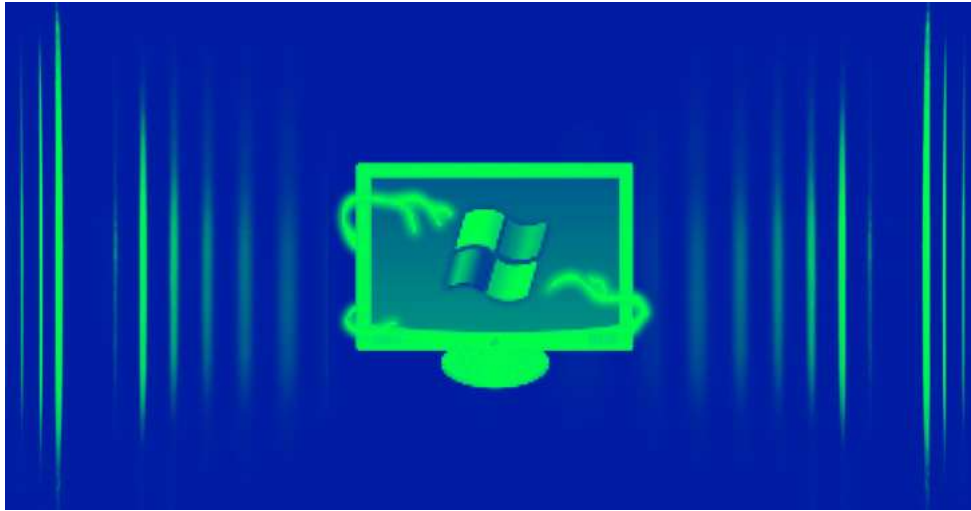


## Researchers Warn of 'Matanbuchus' Malware Campaign Dropping Cobalt Strike Beacons

June 27, 2022 Ravie Lakshmanan



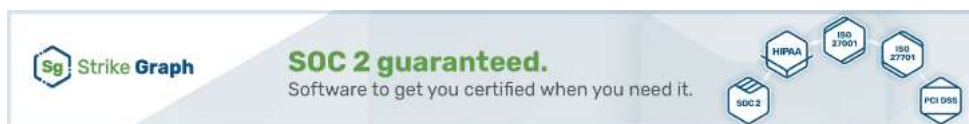
([https://thehackernews.com/new-](https://thehackernews.com/new-images/img/b/R29vZ2xl/AVvXsEjVm8JcLoWlHoUImb_WzqChL0vj2qzq2E9aYaOViPaZf03ya6LqRdh5_fQhiNle_XK8D7LIJEAbEqqLkNgIEfvMebaXoEVKsm39_QM7DXhfZ44BojS0VYECMmYID3BcEgi3jT6xpk/s728-e100/h)

[images/img/b/R29vZ2xl/AVvXsEjVm8JcLoWlHoUImb\\_WzqChL0vj2qzq2E9aYaOViPaZf03ya6LqRdh5\\_fQhiNle\\_XK8D7LIJEAbEqqLkNgIEfvMebaXoEVKsm39\\_QM7DXhfZ44BojS0VYECMmYID3BcEgi3jT6xpk/s728-e100/h](https://thehackernews.com/new-images/img/b/R29vZ2xl/AVvXsEjVm8JcLoWlHoUImb_WzqChL0vj2qzq2E9aYaOViPaZf03ya6LqRdh5_fQhiNle_XK8D7LIJEAbEqqLkNgIEfvMebaXoEVKsm39_QM7DXhfZ44BojS0VYECMmYID3BcEgi3jT6xpk/s728-e100/h)

A malware-as-a-service (Maas) dubbed **Matanbuchus** has been observed spreading through phishing campaigns, ultimately dropping the Cobalt Strike post-exploitation framework on compromised machines.

Matanbuchus, like other [malware loaders](https://flashpoint.io/blog/malware-loaders-continue-to-evolve-proliferate/) (https://flashpoint.io/blog/malware-loaders-continue-to-evolve-proliferate/) such as [BazarLoader](https://thehackernews.com/2022/02/notorious-trickbot-malware-gang-shuts.html) (https://thehackernews.com/2022/02/notorious-trickbot-malware-gang-shuts.html) , [Bumblebee](https://thehackernews.com/2022/04/cybercriminals-using-new-malware-loader.html) (https://thehackernews.com/2022/04/cybercriminals-using-new-malware-loader.html) , and [Colibri](https://thehackernews.com/2022/04/researchers-uncover-how-colibri-malware.html) (https://thehackernews.com/2022/04/researchers-uncover-how-colibri-malware.html) , is engineered to download and execute second-stage executables from command-and-control (C&C) servers on infected systems without detection.

Available on Russian-speaking cybercrime forums for a price of \$2,500 since February 2021, the malware is equipped with capabilities to launch .EXE and .DLL files in memory and run arbitrary PowerShell commands.



(<https://go.thn.li/strike-d>)

The findings, released by threat intelligence firm Cyble last week, document the latest infection chain associated with the loader, which is linked to a threat actor who goes by the online moniker BelialDemon.

"If we look historically, BelialDemon has been involved in the development of malware loaders," Unit 42 researchers Jeff White and Kyle Wilhoit [noted](https://unit42.paloaltonetworks.com/matanbuchus-malware-as-a-service/) (https://unit42.paloaltonetworks.com/matanbuchus-malware-as-a-service/) in a June 2021 report. "BelialDemon is considered the primary developer of

**TriumphLoader** (<https://bazaar.abuse.ch/browse/tag/TriumphLoader/>) , a loader previously posted about on several forums, and has experience with selling this type of malware."

The spam emails distributing Matanbuchus come with a ZIP file attachment containing an HTML file that, upon opening, decodes the Base64 content embedded in the file and drops another ZIP file on the system.

The archive file, in turn, includes an MSI installer file that displays a fake error message upon execution while stealthily deploying a DLL file ("main.dll") as well as downloading the same library from a remote server ("telemetrysystemcollection[.]com") as a fallback option.

"The main function of dropped DLL files ('main.dll') is to act as a loader and download the actual Matanbuchus DLL from the C&C server," Cyble researchers [said](https://blog.cyble.com/2022/06/23/matanbuchus-loader-resurfaces/) (<https://blog.cyble.com/2022/06/23/matanbuchus-loader-resurfaces/>) , in addition to establishing persistence by means of a [scheduled task](https://blog.qualys.com/vulnerabilities-threat-research/2022/06/20/defending-against-scheduled-task-attacks-in-windows-environments) (<https://blog.qualys.com/vulnerabilities-threat-research/2022/06/20/defending-against-scheduled-task-attacks-in-windows-environments>) .

For its part, the Matanbuchus payload establishes a connection to the C&C infrastructure to retrieve next-stage payloads, in this case, two Cobalt Strike Beacons for follow-on activity.




(<https://go.thn.li/crowd-mid-d>)

The development comes as researchers from Fortinet FortiGuard Labs disclosed a new variant of a malware loader called IceXLoader that's programmed in Nim and is being marketed for sale on underground forums.

Featuring abilities to evade antivirus software, phishing attacks involving IceXLoader have paved the way for **DarkCrystal RAT** (<https://thehackernews.com/2022/05/experts-sound-alarm-on-dcrat-backdoor.html>) (aka DCRat) and rogue cryptocurrency miners on hacked Windows hosts.

"This need to evade security products could be a reason the developers chose to transition from AutoIt to Nim for IceXLoader version 3," the researchers [said](https://www.fortinet.com/blog/threat-research/new-icexloader-3-0-developers-warm-up-to-nim) (<https://www.fortinet.com/blog/threat-research/new-icexloader-3-0-developers-warm-up-to-nim>) . "Since Nim is a [relatively uncommon language](https://thehackernews.com/2021/07/hackers-turning-to-exotic-programming.html) (<https://thehackernews.com/2021/07/hackers-turning-to-exotic-programming.html>) for applications to be written in, threat actors take advantage of the lack of focus on this area in terms of analysis and detection."

Found this article interesting? Follow THN on [Facebook](https://www.facebook.com/thehackernews) (<https://www.facebook.com/thehackernews>) , [Twitter](https://twitter.com/thehackersnews)  (<https://twitter.com/thehackersnews>) and [LinkedIn](https://www.linkedin.com/company/thehackernews/) (<https://www.linkedin.com/company/thehackernews/>) to read more exclusive content we post.