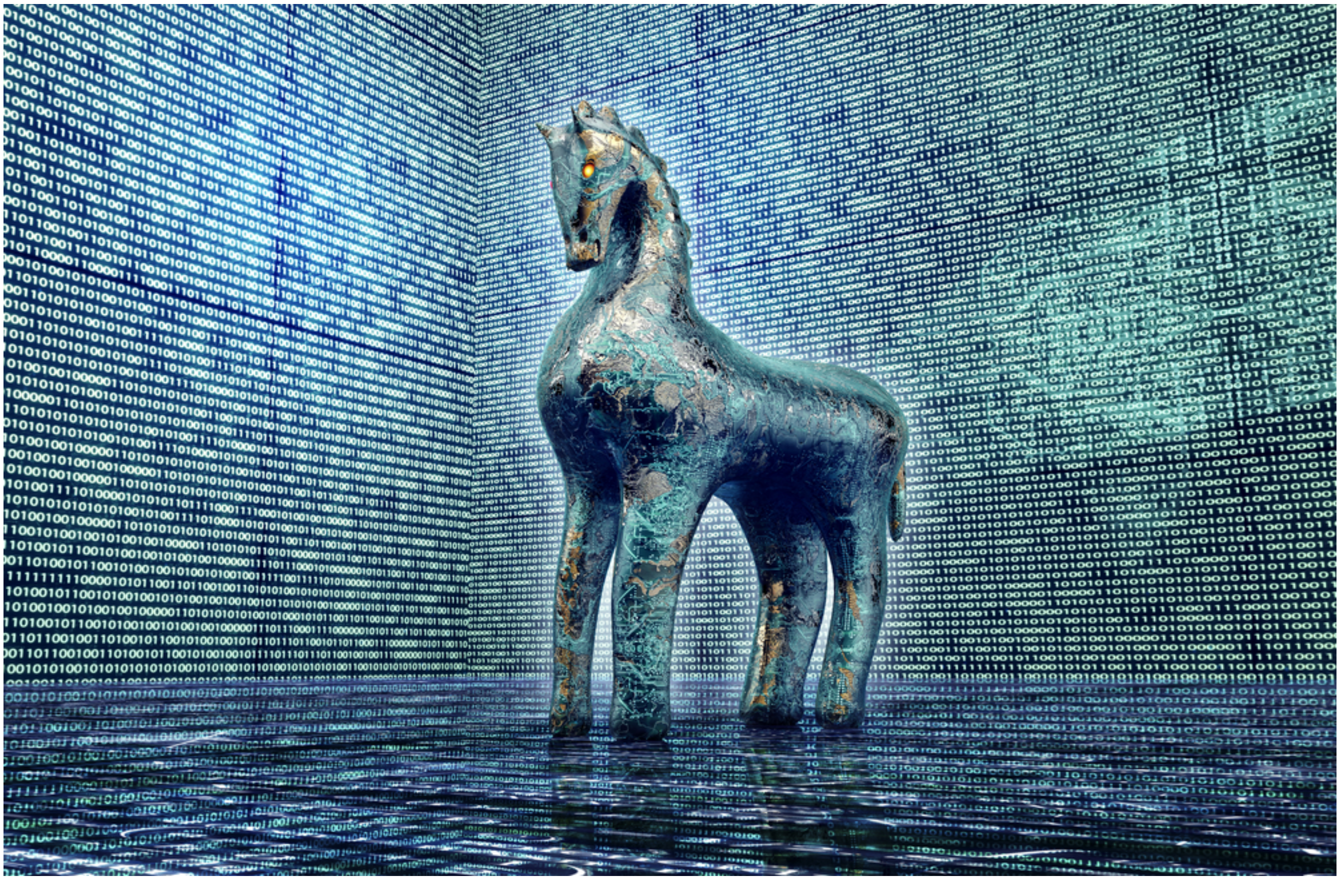
Deep dive into the Pikabot cyber threat

news.sophos.com/en-us/2023/06/12/deep-dive-into-the-pikabot-cyber-threat/

Karl Ackerman

June 12, 2023



Pikabot is a recently discovered malware trojan and with the June update to Sophos NDR, we have added an additional machine learning model to detect the encrypted traffic pattern of suspect Pikabot communication. This detection capability has already been deployed to the Sophos NDR sensors, and no additional updates are required.

How Pikabot works

As a malware trojan, Pikabot is modular, composed of two main components: a loader and a core module. The core module executes the majority of the malware's functions, while the loader assists in carrying out these malicious activities.[1].[2].

Pikabot operates as a backdoor, enabling unauthorized remote access to compromised systems. It receives commands from a command-and-control (C2) server, which can range from injecting arbitrary shellcode, DLLs, or executable files, to distributing other malicious tools such as Cobalt Strike. This suggests that Pikabot could be a potent player in multi-staged attacks.

The commands it can execute are diverse, including running shell commands, fetching and running EXE or DLL files, sending additional system information, altering the C2 check-in interval, and even a "destroy" command which is currently not implemented.[1].

Distribution

Early analysis led researchers to believe that Pikabot was distributed by the Qakbot trojan. However, further study revealed that Pikabot's distribution methods mirror those of Qakbot. The exact distribution methods remain somewhat of a mystery, but clear parallels with known Qakbot campaigns have been identified.[1].

Pikabot's modus operandi

Pikabot's modular structure allows it to carry out various malicious activities. Although the loader component has limited functionality, the core module is where the real action happens. Pikabot deploys an injector to run anti-analysis tests before decrypting and injecting the core module payload. If any of these tests fail, Pikabot aborts its execution, making it difficult for researchers to analyze and understand its actions.

In terms of anti-analysis techniques, Pikabot checks for the presence of debuggers, breakpoints, and system information. It uses public tools like ADVobfuscator for string obfuscation and has numerous methods to detect sandbox environments, debugging, and other analysis attempts.

The core module payload is cleverly encrypted and stored in PNG images. These images are decrypted using a hardcoded 32-byte key, and the decrypted data is further processed using AES (CBC mode). The payload is then injected into a specified process like WerFault, with Pikabot setting certain flags to protect the injected process from non-signed Microsoft binaries.[2].

Interesting findings

One of the intriguing features of Pikabot is its self-termination if the system's language is Georgian, Kazakh, Uzbek, or Tajik. This suggests that the authors may be deliberately avoiding systems in specific geographic regions. Furthermore, Pikabot appears to be in the early stages of development as suggested by its version number (0.1.7) found in its initial communication with the C2 server.[2].

There are also striking similarities between Pikabot and another malware family, Matanbuchus. Both are written in C/C++, utilize a loader/core component split, employ JSON+Base64+crypto for traffic, and extensively use hardcoded strings. These similarities hint at a potential connection between the two malware families.[1].

Pikabot C2 infrastructure

With the June 2023 update to Sophos NDR, we added a CNN model to detect Pikabot and have already discovered a number of new C2 servers:

IP	PORT	Virus Total	JARM
192[.]9[.]135[.]73	1194	Link	21d19d00021d21d21c21d19d21d21dd188f9fdeea4d1b361be3a6ec494b2d2
185[.]87[.]148[.]132	1194	Link	21d19d00021d21d21c21d19d21d21dd188f9fdeea4d1b361be3a6ec494b2d2
45[.]154[.]24[.]57	2078	Link	21d19d00021d21d21c21d19d21d21dd188f9fdeea4d1b361be3a6ec494b2d2
45[.]85[.]235[.]39	2078	Link	21d19d00021d21d21c21d19d21d21dd188f9fdeea4d1b361be3a6ec494b2d2
129[.]153[.]135[.]83	2078	Link	21d19d00021d21d21c21d19d21d21dd188f9fdeea4d1b361be3a6ec494b2d2
193[.]122[.]200[.]171	2078	Link	21d19d00021d21d21c21d19d21d21dd188f9fdeea4d1b361be3a6ec494b2d2
104[.]233[.]193[.]227	2078	Link	21d19d00021d21d21c21d19d21d21dd188f9fdeea4d1b361be3a6ec494b2d2
94[.]199[.]173[.]6	2222	Link	21d19d00021d21d21c21d19d21d21dd188f9fdeea4d1b361be3a6ec494b2d2
132[.]148[.]79[.]222	2222	Link	21d19d00021d21d21c21d19d21d21dd188f9fdeea4d1b361be3a6ec494b2d2

IP	PORT	Virus Total	JARM
38[.]54[.]33[.]239	2222	Link	21d19d00021d21d21c21d19d21d21dd188f9fdeea4d1b361be3a6ec494b2d2
144[.]172[.]126[.]136	2222	Link	21d19d00021d21d21c21d19d21d21dd188f9fdeea4d1b361be3a6ec494b2d2
129[.]80[.]164[.]200	32999	Link	21d19d00021d21d21c21d19d21d21dd188f9fdeea4d1b361be3a6ec494b2d2
129[.]153[.]22[.]231	32999	Link	21d19d00021d21d21c21d19d21d21dd188f9fdeea4d1b361be3a6ec494b2d2

NOTE: The VirusTotal information for Sophos detections is delayed