China Chopper

By Contributors to Wikimedia projects

Published: 2019-03-10 · Archived: 2026-04-05 21:22:50 UTC

From Wikipedia, the free encyclopedia

China Chopper is a web shell approximately 4 kilobytes in size, first discovered in 2012. This web shell is commonly used by malicious Chinese actors, including advanced persistent threat (APT) groups, to remotely control web servers. This web shell has two parts, the client interface (an executable file) and the receiver host file on the compromised web server.

China Chopper has many commands and control features such as a password brute-force attack option, code obfuscation, file and database management and a graphical user interface.[1][2][3][4] It originally was distributed from a website www.maicaidao.com which is now down. FireEye revealed that the client of this web shell is programmed in Microsoft Visual C++ 6.0

China Chopper was used in attacks against eight Australian web hosting providers which were compromised due to their use of an unsupported operating system (Windows Server 2008). Hackers connected the web servers to a Monero mining pool, by which they mined about 3868 AUD worth of Monero.[5]

In 2021, a version of the web shell programmed in JScript was used by Advanced Persistent Threat group Hafnium to exploit four zero-day vulnerabilities in Microsoft Exchange Server, in the 2021 Microsoft Exchange Server data breach. This web shell was dropped when one of these vulnerabilities was exploited, allowing attackers to upload a program which ran with administrator privileges.[6] With only the address of the .aspx file containing the script, a HTTP POST request could be made to the script with just a command in the request, causing the script to execute the command immediately using the JScript 'eval' function, allowing attackers to run arbitrary code on the server.[7]

1. ^ *"China Chopper"*. *NJCCIC*. *Archived from the original on 13 January 2019. Retrieved 22 December 2018.*
2. ^ *"What is the China Chopper Webshell, and how to find it on a compromised system?"*. *28 March 2018. Archived from the original on 13 January 2019. Retrieved 22 December 2018.*
3. ^ *"Breaking Down the China Chopper Web Shell - Part I « Breaking Down the China Chopper Web Shell - Part I"*. *Mandiant*. *Archived from the original on 13 January 2019. Retrieved 2022-01-03.*
4. ^ *"Breaking Down the China Chopper Web Shell - Part II « Breaking Down the China Chopper Web Shell - Part II"*. *Mandiant*. *Archived from the original on 7 January 2019. Retrieved 2022-01-03.*
5. ^ *Stilgherrian*. *"Australian web hosts hit with a Manic Menagerie of malware"*. *ZDNet*. *Archived from the original on 2019-01-31. Retrieved 2019-03-17.*
6. ^ *"ProxyLogon"*. *ProxyLogon (in Chinese (Taiwan)). Retrieved 2021-03-16.*
7. ^ *"Exchange Cyberattacks Escalate as Microsoft Rolls One-Click Fix"*. *threatpost.com. 16 March 2021. Retrieved 2021-03-16.*