



HC3: Analyst Note

November 12, 2024 TLP:CLEAR Report: 202411121500

Godzilla Webshell

Executive Summary

Godzilla webshell is a weapon used by cyber threat actors to execute commands, manipulate files, and engage in other harmful and malicious activity on victim systems as part of a larger cyberattack. It has been attributed to Chinese state threat actors with relatively high confidence, and has been used to target a number of industries, including the health sector. It is publicly available and therefore accessible for use by any number of bad actors, and should be treated as a serious threat. This article concludes with defense and mitigation recommendations, which we implore all healthcare organizations to review and action in accordance with their risk mitigation plan.

What is Godzilla?

Godzilla [webshell](#) is a Chinese-language backdoor created by an individual who goes by the online handle BeichenDream. BeichenDream claims Godzilla was created in response to existing webshells that are often detected in attacks; Godzilla avoids detection by using Advanced Encryption Standard encryption for its network traffic, which makes it more difficult to detect. Godzilla is considered highly capable and full of functionality. It facilitates file management and manipulation, including uploading, downloading, deleting, and modifying files on a victim system. It also allows the execution of files and commands—one of the primary functions of any webshell. It allows for reconnaissance, such as the collection of details related to operating systems, network configurations, and versions of software and applications. It facilitates the maintenance of persistent access. As previously noted, it is capable of encryption. It also executes in memory, or “filelessly”, which also makes it challenging to detect. There are a number of reports that attribute Godzilla to the Chinese government. We recommend that this be understood as probable, but not certain. It is also worth noting that BeichenDream maintains Godzilla, including its code, on a publically accessible repository. This means it is relatively trivial for another threat actor—foreign government, cybercriminal gang or anyone else—to acquire, modify, and utilize the code in accordance with their unique purposes.

Known Attack Campaigns

We are aware of the following noteworthy cyberattacks and attack campaigns leveraging Godzilla:

- In November 2021, the U.S. Department of Homeland Security’s (DHS) Cybersecurity and Infrastructure Security Agency (CISA) [reported](#) on Advanced Persistent Threat (APT) actors leveraging Godzilla in [a series of attacks](#) exploiting a known authentication bypass vulnerability (CVE-2021-40539) in ManageEngine ADSelfService Plus, a self-service password management and single sign-on platform.
- Also in November 2021, both Microsoft and Palo Alto identified a second, related campaign leveraging Godzilla, exploiting the same vulnerability as above. These attacks were [attributed by Microsoft](#) to a group they identify as DEV-0322, a group which they report is operating out of China (based on observed infrastructure, victimology, tactics, and procedures). [Palo Alto’s reporting](#) noted the use of leased infrastructure in the United States to carry out these attacks. This campaign was [reported to have targeted the health sector](#).
- In February of 2023, ASEC [reported](#) on an attack campaign carried out by the APT Dalbit (also known as m00nlight), targeting victims with Godzilla (as well as other weapons). These attacks cut across many industries, involved a number of tactics, techniques and procedures (TTPs) and incorporated several weapons. A high-level diagram of the campaign can be seen in **Figure 1**.



HC3: Analyst Note

November 12, 2024 TLP:CLEAR Report: 202411121500

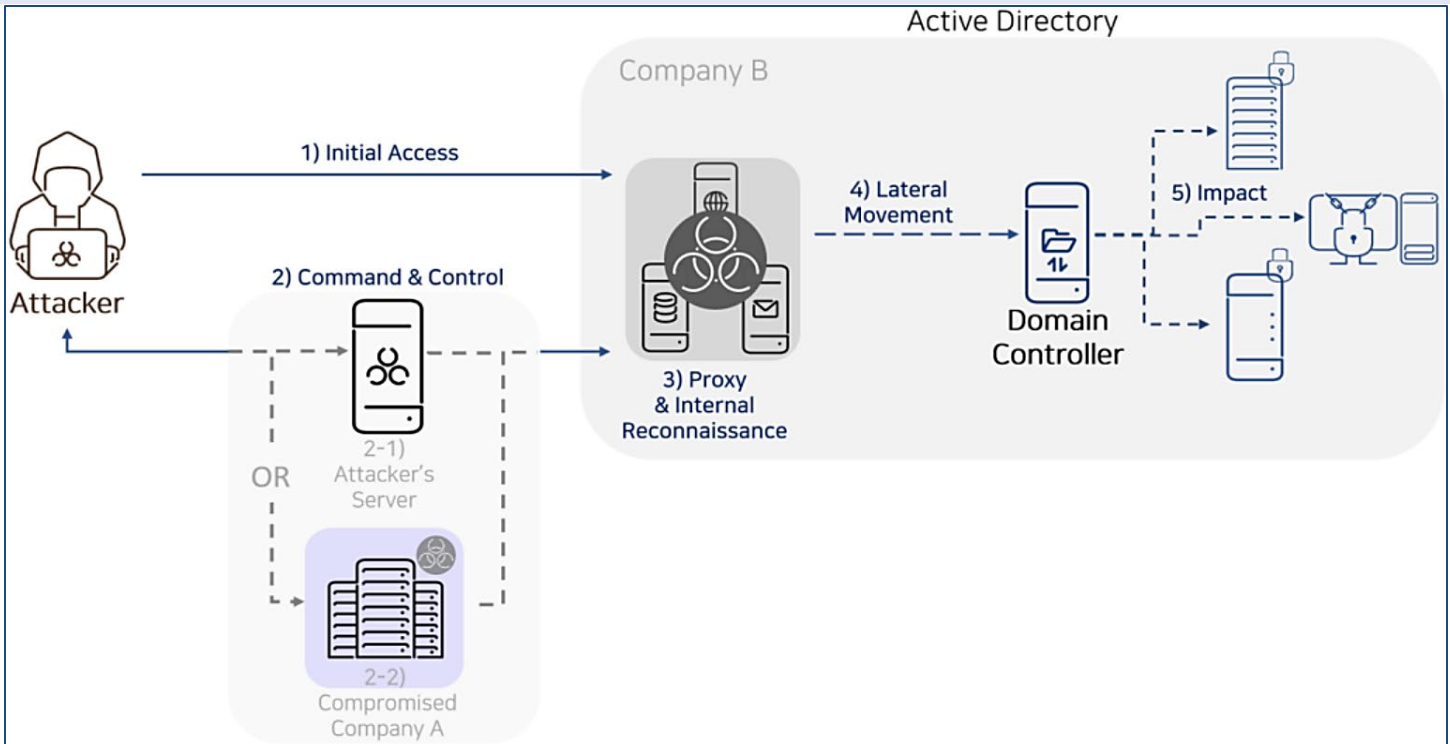


Figure 1: A high-level diagram of an attack campaign leveraging Godzilla as reported in February 2023. (Image source: <https://asec.ahnlab.com/en/47455/>)

Prevention, Detection, and Mitigation

Due to the high functionality and continuous development of Godzilla, it is not practical to attempt to compile a list of defense and mitigation steps to be implemented over any long period of time. However, we do recommend a report from [CISA](#) detailing a campaign leveraging Godzilla, as well as generic webshell defensive resources from [the National Security Agency](#), [Group-IB](#), and [Imperva](#).

[Yara](#) rules for Godzilla can be found [here](#) and [here](#). Indicators of Compromise can be found here:

- <https://www.microsoft.com/en-us/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/>
- <https://unit42.paloaltonetworks.com/manageengine-godzilla-nlite-kdc.sponge/>
- <https://asec.ahnlab.com/en/47455/>

References

Zoho's ManageEngine Password Manager Flaw Torched by Godzilla Webshell
<https://threatpost.com/zoho-password-manager-flaw-godzilla-webshell/176063/>

Dalbit (m00nlight): Chinese Hacker Group's APT Attack Campaign
<https://asec.ahnlab.com/en/47455/>

