Subject: Chinese Hackers Use New Technique to Infiltrate European Ministries
Posted by admin on Thu, 30 Jul 2026 08:08:46 GMT
View Forum Message <> Reply to Message

Chinese Hackers Use New Technique to Infiltrate European Ministries

"Here's How to Protect Yourself"

Meta Description: Chinese hackers use HTML smuggling to deliver malicious payloads to European ministries. Learn how to protect yourself from this new and emerging threat.

HTML-smuggling

Jul 4, 2023

A group of Chinese hackers has been using a new technique to infiltrate European ministries, according to a report by Check Point Research. The hackers are using a technique called HTML smuggling to deliver malicious payloads inside HTML documents.
What is HTML smuggling?

HTML smuggling is a technique that allows attackers to bypass security filters by embedding malicious code in the data attributes of HTML elements. This code is then executed when the document is opened in a web browser.

The data attributes of HTML elements are used to store additional information about the element, such as its size, color, or position. This information is typically not visible to the user, but it can be accessed by attackers who know how to exploit the vulnerability.
How do the Chinese hackers use HTML smuggling?

The Chinese hackers are using HTML smuggling to deliver a new variant of the PlugX remote access trojan. PlugX is a modular malware that can be used for a variety of purposes, including espionage and data theft.

The hackers are targeting Foreign Affairs ministries and embassies in Europe. They are sending spear-phishing emails that contain malicious HTML documents. When the documents are opened, the malicious code is executed and the PlugX trojan is installed on the victim's computer.

The Check Point researchers have identified two infection chains that are used by the hackers. In one chain, the malicious code deploys a malicious LNK file inside a ZIP file. In the other chain, the malicious code fetches an MSI file from a remote server.
How to protect yourself from HTML smuggling attacks

There are a number of steps that organizations can take to protect themselves from HTML smuggling attacks. These include:

Use a security solution that can detect and block HTML smuggling attacks. There are a number of security solutions available that can detect and block HTML smuggling attacks. These solutions typically use a combination of techniques, such as signature-based detection, behavioral

analysis, and sandboxing.

Train employees to be aware of the threat and to be careful about opening suspicious emails. Employees should be trained to be aware of the HTML smuggling threat and to be careful about opening suspicious emails. They should also be trained to report any suspicious emails to IT security staff.

Keep web browsers and operating systems up to date with the latest security patches. Software vendors typically release security patches to address vulnerabilities that can be exploited by HTML smuggling attacks. Organizations should keep their web browsers and operating systems up to date with the latest security patches to help protect themselves from these attacks.

Additional information

In addition to the steps listed above, organizations can also take the following measures to protect themselves from HTML smuggling attacks:

Use a web browser that has been patched for known HTML smuggling vulnerabilities. Some web browsers have been patched for known HTML smuggling vulnerabilities. Organizations should use a web browser that has been patched for these vulnerabilities to help protect themselves from these attacks.

Enable Content Security Policy (CSP) in web browsers. CSP can help to prevent malicious code from being executed in HTML documents. Organizations should enable CSP in their web browsers to help protect themselves from these attacks.

Use a firewall that can block malicious traffic. A firewall can be used to block malicious traffic that is associated with HTML smuggling attacks. Organizations should use a firewall that can block this traffic to help protect themselves from these attacks.

Conclusion

HTML smuggling is a new and emerging threat that organizations need to be aware of. By taking the steps outlined in this article, organizations can help to protect themselves from this threat.
Updates

Since this article was written, there have been additional developments in the HTML smuggling threat landscape. For example, researchers have discovered new ways that attackers can exploit HTML smuggling to deliver malicious payloads.

Organizations should stay up-to-date on the latest developments in the HTML smuggling threat landscape by subscribing to security mailing lists and following security blogs.

Organizations should also regularly review their security policies and procedures to ensure that they are taking all necessary steps to protect themselves from HTML smuggling attacks.

Extra Tags:

HTML smuggling, Chinese hackers, European ministries, PlugX remote access trojan, Spear-phishing emails, Malicious payloads, Content Security Policy (CSP)