BLACKSWAN
CYBERSECURITY

THREAT ADVISORY

April 4, 2025

Emerging Threat: Invisible Unicode Phishing Attacks

Overview

Cybercriminals are continually evolving their tactics to bypass security measures, and a new phishing attack leveraging an advanced JavaScript obfuscation technique is raising alarms. Researchers at Juniper Threat Labs recently identified this sophisticated method, which uses invisible Unicode characters to conceal malicious JavaScript payloads.

Unmasking the Attack

In early January 2025, affiliates of a major American political action committee (PAC) were targeted using a phishing attack that employed a novel JavaScript obfuscation method. Originally demonstrated by security researcher Martin Kleppe in October 2024, this technique quickly transitioned from a proof of concept into an active threat.

The obfuscation method works by encoding JavaScript payloads using Hangul half-width (U+FFA0) and Hangul full-width (U+3164) Unicode characters, effectively rendering the malicious script invisible. Attackers store the obfuscated code as a property within a JavaScript object. A short bootstrap script retrieves and executes the hidden payload by converting the Hangul characters back into binary via a JavaScript Proxy 'get() trap.'

Advanced Evasion Techniques

Beyond obfuscation, attackers employed several additional techniques to evade detection:

- **Personalized Targeting:** Leveraging non-public information to enhance credibility.
- **Debugger & Timing Checks:** The script detects analysis attempts and redirects to a benign site if debugging is detected.
- **Obscured Phishing Links:** Recursively wrapped Postmark tracking links hide the actual phishing destination.

These techniques make detection and mitigation challenging, as security scanners may overlook the empty whitespace containing the malicious code. Additionally, the obfuscated payload can be injected into legitimate scripts without immediate suspicion.

Implications and Future Risks

The use of this JavaScript obfuscation technique marks a new frontier in phishing attacks. Security researchers have linked some domains involved in this campaign to the Tycoon 2FA phishing kit, suggesting that this method could soon be adopted by a broader range of cybercriminals.

Protecting Against Emerging Threats

With attackers continually refining their methods, organizations must enhance their security posture:

- **Advanced Threat Detection:** Update security tools to recognize obfuscated JavaScript techniques.
- **Security Awareness Training:** Educate employees on identifying and avoiding phishing attempts.
- **Robust Email Security Policies:** Implement filtering mechanisms to prevent malicious scripts from reaching users.

Blackswan Cybersecurity remains committed to monitoring these evolving threats and equipping organizations with the knowledge and tools needed to stay ahead of cybercriminals. Stay vigilant, stay informed, and fortify your defenses against the invisible threats lurking in the digital landscape.

References

- https://www.bleepingcomputer.com/news/security/phishing-attack-hides-javascript-using-invisible-unicode-trick/
- https://blog.knowbe4.com/alert-phishing-attacks-use-new-javascript-obfuscation-technique