UAT-8099: Chinese-speaking cybercrime group targets high-value IIS for SEO fraud

Cisco Talos is disclosing details on UAT-8099, a Chinese-speaking cybercrime group mainly involved in search engine optimization (SEO) fraud and theft of high-value credentials, configuration files, and certificate data. Cisco s file census and DNS analysis show affected Internet Information Services (IIS) servers in India, Thailand, Vietnam, Canada, and Brazil, targeting organizations such as universities, tech firms and telecom providers. UAT-8099 manipulates search rankings by focusing on reputable, high-value IIS servers in targeted regions. The group maintains persistence and alters SEO rankings using web shells, open-source hacking tools, Cobalt Strike, and various BadIIS malware; their automation scripts are customized to evade defenses and hide activity. Talos found several new BadIIS malware samples in this campaign on VirusTotal this year one cluster with very low detection and another containing simplified Chinese debug strings. In April 2025, Cisco Talos identified a Chinese-speaking cybercrime group, tracked as UAT-8099, which targets a broad range of vulnerable IIS servers across specific regions. This group focuses on high-value IIS servers that have a good reputation within these areas to manipulate search engine results for financial gain. UAT-8099 operates as a cybercrime group conducting SEO fraud. Additionally, UAT-8099 uses Remote Desktop Protocol (RDP) to access IIS servers and search for valuable data such as logs, credentials, configuration files and sensitive certificates, which they package for possible resale or further exploitation. Upon discovering a vulnerability in a target server, the group uploads a web shell to collect system information and conduct reconnaissance on the host network. They then enable the guest account, escalate its privileges to administrator level, and use this account to enable RDP. For persistence, they combine RDP access with SoftEther VPN, EasyTier (a decentralized virtual private network tool) and FRP reverse proxy tool. Subsequently, the group performs further privilege escalation using shared tools to gain system-level permissions and install BadIIS malware. To secure their foothold, they deploy defense mechanisms to prevent other threat actors from compromising the same server or disrupting their setup. This blog post provides a comprehensive overview of the campaign s victimology, including the regions affected and the potential consequences of BadIIS infections. It also details the attack chain, automation scripts employed, and the malware and shared hacking tools UAT-8099 commonly uses. Victimology Based on Cisco's file census and DNS traffic analysis, the affected IIS server regions include India, Thailand, Vietnam, Canada and Brazil. The targeted IIS servers are owned by organizations such as universities, technology companies and telecommunications providers. The compromised IIS servers redirect users to unauthorized advertisements or illegal gambling websites. The languages used on these websites assists with identifying the targeted regions or countries. While Talos observed that most victims were located within the same region as the compromised servers, some victims were affected when accessing compromised servers in different regions. Figure 1. Gambling websites in Thai, Portuguese and English. The majority of their targets are mobile users, encompassing not only Android devices but also Apple iPhone devices. Figure 2. Gambling Android Package Kit (APK) download site. Figure 3. Gambling iOS app download site. Attack chain In this campaign, the UAT-8099 group took advantage of weak settings in the web server s file upload feature. Figure 4. UAT-8099 attack chain flowchart. The target web server allowed users to upload files to the server, but did not restrict the file type, which allowed UAT-8099 to upload the web shell. This established initial access and gave them control over the compromised server. The following is the detected location of the web shell used in this campaign, which is identified as the open-source ASP.NET Web BackDoor web shell: C:/inetpub/wwwroot/[REDACTED]/Html/hw/server.ashx After dropping the web shell, Talos observed the actor utilizing it to execute commands such as ipconfig, whoami, arp and tasklist to collect system information and discover the host network information. Once the collection of information is complete, UAT-8099 enables the guest account, setss a password, and elevate the guest user privileges to administrator level, including the ability to access the system using RDP. Then, the actor uses another command to identify the network ports on which the TermService (Remote Desktop Services) process is actively listening. After completing creating a guest account and enabling the RDP on that target IIS server, the actor created a hidden account admin$ and added it to Administrator permission privilege for long-term persistence.

Command	MITRE
cmd /c net user guest / active:yes & net user guest P@ssw0rd & net localgroup administrators guest /add & net localgroup Remote Desktop Users guest /add	T1136.001
cmd /c cd /d C:/Windows/SysWOW64/inetsrv/&for /f tokens=2 % i in ('tasklist /FI SERVICES eq TermService /NH') do netstat - ano | findstr % i | findstr LISTENING 2>&1	T1049 T1007 T1057

cmd
/c net user admin$ P@ssw0rd /add T1136.001
cmd
/c net localgroup Administrators admin$ /add T1098
cmd.exe
/C net user test [REDACTED] /add T1136.001
cmd.exe
/C net localgroup administrators test /add T1098 Table 1.
Initial access,
reconnaissance and addition of user credentials. To maintain access to the target IIS server and install the BadIIS malware for SEO fraud, Talos observed the actor completing three steps to achieve
persistence, escalate privileges, install malware and build a self-defense solution: UAT-8099 is deploying SoftEther VPN, EasyTier (a decentralized virtual private
network tool) and fast reverse
proxy (FRP). This setup enabled them to use RDP remotely to
control
the server. The actor also leveraged a shared public tool to escalate privileges on the IIS server. They then used
Procdump
to extract
victim credentials, which were subsequently compressed with WinRAR. We assess that these actions were taken to finalize the installation of BadIIS for their SEO fraud activities. The actor installed D_Safe_Manage , a well-known Windows IIS security tool, to prevent other attackers from compromising the server and tampering with their BadIIS setup. Command
MITRE
cmd
/c C:/Users/Public/Libraries/install_VPN.bat T1059.003
C:\
Users\Public\Libraries\mass
.exe -c
C:\
Users\Public\Libraries\config.yaml T1133
cmd.exe
/C frpc
.exe -c frpc.ini T1133
cmd

/c C:/Users/Public/Music/mess
.exe /install T1133
C:\
Users\Public\Videos\a
.exe T1548
C:\
Users\Public\Videos\D_Safe_Manage
.exe N/A C:/Users/Public/Videos/xmiis32.dll T1496
C:/Users/Public/Videos/xmiis64.dll T1496 C:/Users/admin$/Desktop/
procdump.exe
- accepteula -ma
lsass.exe
lsass
.dmp T1003
C:\
Program Files\WinRAR\WinRAR
.exe a -ep1 - scul -r0 - iext
-- Videos.rar
C:\
Users\Public\Videos\system.hive
C:\
Users\Public\Videos\sam.hive T1560 Table 2. Installation of tools, dumping user credentials for exfiltration and securing the installation. Talos did not only observe UAT-8099 conducting SEO fraud, but also stealing high-value credentials, configuration files and certificate data. After successfully compromising the target IIS server and deploying their BadIIS tool, their next step was to search for valuable credentials, configuration files, and certificate data within the compromised system. The commands Talos observed indicate the actor utilizes RDP to access the IIS server. Once inside, they leverage the 'Everything' graphical user interface (GUI) tool a fast filename search engine for Windows to locate high-value data such as logs, credentials, configuration files and sensitive certificates. Upon identifying relevant files, the actor used Notepad to review the content and employed Windows Crypto Shell Extensions (via
rundll32.exe
cryptext.dll) to open and inspect .crt certificate files, examining their properties and details. Finally, all collected high-value files were

consolidated into a hidden directory, specifically Users\admin$\Desktop\loade\ . These files were then archived using WinRAR before being exfiltrated to the actor. Command MITRE

```
C:\
Users\admin$\Desktop\Everything
.exe -enable-run-as-admin T1083
C:\
Windows\
system32
\NOTEPAD
.EXE
C:\
[ REDACTED]Log\10-09-2024.txt T1005
C:\
Windows\
system32
\NOTEPAD
.EXE
C:\
[ REDACTED]Log\19-03-2025.txt T1005
C:\
Windows\
system32
\NOTEPAD
.EXE E:\[ REDACTED]- csr \[REDACTED]-csr.txt T1649
C:\
Windows\
system32
\
rundll32.exe
cryptext.dll,CryptExtOpenCER E:\.[ REDACTED]- csr
\STAR_[REDACTED]\AAACertificateServices.crt T1649
C:\
Windows\
system32
\
rundll32.exe
cryptext.dll,CryptExtOpenCER E:\.[ REDACTED]- csr
\STAR_[REDACTED]\SectigoRSADomainValidationSecureServerCA.crt T1649
```

```
C:\
Windows\
system32
\
rundll32.exe
cryptext.dll,CryptExtOpenCER E:\.[ REDACTED]- csr
\STAR_[REDACTED]\STAR_[REDACTED].crt T1649
C:\
Windows\
system32
\
rundll32.exe
cryptext.dll,CryptExtOpenCER E:\.[ REDACTED]- csr
\STAR_[REDACTED]\USERTrustRSAAAACA.crt T1649
C:\
Windows\
system32
\
rundll32.exe
cryptext.dll,CryptExtOpenCER E:\AAACertificateServices.crt T1649
C:\
Windows\
system32
\
rundll32.exe
cryptext.dll,CryptExtOpenCER
E:\SectigoRSADomainValidationSecureServerCA.crt T1649
C:\
Windows\
system32
\
rundll32.exe
cryptext.dll,CryptExtOpenCER E:\USERTrustRSAAAACA.crt T1649
C:\
Windows\
system32
\NOTEPAD
.EXE
C:\
Users\ admissionportal \Desktop\[ REDACTED]_DB_UPDATE.txt T1528
C:\
Program Files\Notepad++\notepad++
.exe
C:\
Users\Administrator\.gitconfig T1528
C:\
Program Files\Notepad++\notepad++
.exe
C:\
Users\Administrator\.
aws\config T1528
C:\
Program Files\Notepad++\notepad++
.exe
C:\
Users\Administrator\.
aws\credentials T1649
C:\
Windows\
system32
\NOTEPAD
.EXE
C:\
Users\Administrator\OneDrive - [REDACTED] \website\[ REDACTED]-website \.
gitignore T1528
C:\
Program Files\Notepad++\notepad++
.exe
C:\
Users\Administrator\
AppData
\Roaming\S3Browser\accounts.xml T1528
C:\
Windows\
system32
\NOTEPAD
.EXE
C:\
Windows\debug\PASSWD.LOG T1528
C:\
Windows\
system32
\NOTEPAD
.EXE
C:\
inetpub \ wwwroot \Html-[ REDACTED]\Html\images\passwd_web.xml T1528
C:\
Windows\
system32
\NOTEPAD
.EXE
C:\
Users\[ REDACTED]\
AppData
\Local\Google\Chrome\ d_emxqyvq \ ZxcvbnData \3\passwords.txt T1528
C:\
Windows\
system32
\NOTEPAD
.EXE
C:\
Users\admin$\
AppData
\Roaming\S3Browser\logs\s3browser-win32-2025-04-24-log.txt T1528
C:\
Windows\
system32
\NOTEPAD
.EXE
C:\
Users\admin$\
AppData
\Roaming\S3Browser\
s3 browser.settings-v3 T1 528
C:\
Program Files\WinRAR\WinRAR
.exe x - iext -ow - ver
```

--

C:\

Users\admin$\Desktop\loade.zip

C:\

Users\admin$\Desktop\loade\ T1560 Table 3. Searching and preparing credentials and certificates for exfiltration. Automation script used Talos also observed UAT-8099 dropping and executing three batch script files in some attacks to automate their tasks or to set up the compromised server for persistence and SEO fraud. The first script is for IIS module installation, as documented in Talos DragonRank and Trend Micro blog posts.

C:\

Windows\

system32

\

cmd.exe

/c

C:\

ProgramData

\iis.bat Figure 5. Setting up the server for persistence and SEO fraud. The second script is for configuring RDP settings and related network activity on a Windows system, including past RDP usage, the RDP listening port, the status of the RDP service, associated network activity, and to configure the Windows firewall to allow RDP.

C:\

Windows\

system32

\

cmd.exe

/c

C:\

ProgramData

\fuck.bat Figure 6. Configuring RDP settings to allow incoming connections. The third set of scripts is designed to establish and immediately trigger a persistent, high privilege scheduled task using inetinfo .exe , and then list all system scheduled tasks. The inetinfo

.exe is a legitimate file WMI V2 provider code generation tool that is used by the actor to do DLL sideloading and run the Cobalt Strike in memory. The detailed Cobalt Strike analysis will be described in the next section.
C:\
Windows\
system32
\
cmd.exe
/c
C:\
ProgramData
\1
.bat Figure 7. inetinfo
.exe is used to sideload a Cobalt Strike
beacon. Talos
observed UAT-8099 utilized Cobalt Strike as their backdoor in this campaign. They employed DLL sideloading as a method to execute the backdoor and also established a scheduled task to maintain
persistence on the
compromised systems. Figure 9. Cobalt Strike
beacon execution diagram. The encrypted first-stage
payload is embedded within the wmicodegen.dll file. When this DLL is loaded by the legitimate WMI V2 provider code generation tool, it uses the
VirtualQuery API to allocate a block of memory specifically for this
first-stage
payload. Figure 10. Uses VirtualQuery API to load first-stage
payload. After decrypting the first stage
payload, we can see both the second stage
payload combined with a small piece of shellcode, and the third stage
payload, which is encrypted and encoded with
Base64
. Figure 11. The second stage
payload. When jumping into the third stage
payload, we
observed it is a DLL file but without the original PE header. We also identify this third stage
payload as the User-Defined Reflective Loader for the Cobalt Strike
beacon. The erased original PE header and heavy obfuscation in each stage are consistent with the blog description . In addition, the machine

information collection structure is also the same as the beacon structure such as listener name, computer name, username and process name. The listener name in this campaign is PUBG. Figure 12. Beacon structure with the listener name PUBG. Most importantly, the DLL file contains the udrl.x64.dll and customLoader inside that also match with the User-Defined Reflective Loader blog description. Using a

URL

that mimics a legitimate content delivery network (CDN), along with ports and paths typical of Exchange servers , enables the attacker to blend in with normal network traffic and avoid detection by security analysts. Figure 13. udrl.x64.dll and customLoader embedded. Figure 14. Beacon C2 connection information. Talos' analysis of the BadIIS variants used in this campaign revealed functional and

URL

pattern similarities to a variant previously documented in the Black Hat USA 2021 white paper and a Trend Micro blog . However, this new BadIIS malware has altered its code structure and functional workflow to evade detection by antivirus products. Additionally, we identified several instances of the BadIIS malware on VirusTotal this year. One cluster exhibited very low detection rates and the other showed simplified Chinese debug strings inside the malware. Figure 15. First cluster of new BadIIS with low detection rates. Figure 16. Second cluster of new BadIIS with simplified Chinese debug strings. The first cluster of new BadIIS malware implements handlers named CHttpModule ::OnBeginRequest and CHttpModule ::OnSendResponse . Both handlers use the "

User-Agent

" and "Referer" fields from the incoming HTTP headers to determine which malicious function to execute. Specifically, this malware targets requests where the "

User-Agent

" is Googlebot and the "Referer" is google.com, confirming that the user and crawler accessed the

compromised website via the Google search engine only. Below, we describe how the malicious functions, including proxy, injector and SEO fraud, trigger. SEO manipulation schemes The OnBeginRequest handler processes incoming requests by examining the " User-Agent " and "Referer" HTTP headers to proxy or Injector responses. When the request is detected as originating from Googlebot and meets a specific URL path condition, the request is forwarded through a Proxy function. The targeted URL path pattern is as follows: news
|cash
|bet
|gambling
|betting
|casino
|fishing
|deposit
|bonus
|sitemap
|app
|ios
|video
|games
|xoso
|dabong
|nohu
|yono
|apks
|android
|hots
|vna
|craps
|banca
|online
|sicbo

|uono
|yono
|cocs
|matkas Alternatively, if the request is not from Googlebot, the system then checks if it was referred by a Google search and if the same

URL

path condition is satisfied, in which case it proceeds to inject JavaScript. The injected JavaScript embeds a
C2

URL

such as http:
//[
C2]/jump.html or http:
//[
C2]/pg888.js . This injection enables the actor to
compromise users browsers by downloading malicious scripts from the
C2 server. Figure 17. OnBeginRequest handler. Figure 18.
Proxy mode. Figure 19. Injector mode. The OnSendResponse handler first performs SEO fraud by delivering specific content from
C2 server to requests where the "

User-Agent

" is Googlebot, manipulating search rankings to increase the visibility of the malicious content. This
C2 content typically appears as a

URL

like http:
//[
C2]/u.php . Subsequently, the function targets human users by conditionally injecting JavaScript when a request comes from a Google search and results in a 404 or 500 error page. Figure 20. OnSendResponse handler. Figure 21.
SEO fraud mode. Technical highlights of each mode
Proxy mode When operating in
proxy mode, BadIIS first verifies the

URL

path to ensure the process is running in the correct mode. It then extracts the embedded
C2 server address, which is encoded in hexadecimal bytes, and uses this
C2 as a
proxy to retrieve content from a secondary

C2 server, subsequently responding to the IIS server. Figure 22. Use C2 server as a proxy. Before responding to the Google crawler, it modifies the response data to resemble a valid HTTP response and uses the native HTTP module API "WriteEntityChunks" to insert data into the body of the HTTP response. Figure 23. Using WriteEntityChunks to insert data into the body of the HTTP response. SEO fraud mode Talos identified that the actor employs a conventional SEO technique known as backlinking to boost website visibility. Google's search engine uses backlinks to discover additional sites and assess keyword relevance. A higher number of backlinks increases the likelihood of Google crawlers visiting a site, which can accelerate ranking improvements and enhance exposure for the webpages. However, simply accumulating backlinks without regard to quality can lead to penalties from Google. Algorithms like Penguin , introduced in 2012, and SpamBrain , launched in 2022, rigorously evaluate backlink quality. To exploit this, the actor compromises multiple IIS servers across the internet to conduct SEO fraud. In this SEO fraud mode, BadIIS serves numerous backlinks with HTML content to Google crawlers to improve search engine rankings. Figure 24. Retrieving backlinks containing HTML content. One example of a backlink from the C2 server is shown in Figure 25, with additional compromised IIS servers performing similar backlink SEO fraud. Figure 25. Backlinks from the C2 server. Injector mode In injector mode, BadIIS intercepts browser requests originating from Google search results. It connects to the C2 server to retrieve JavaScript code, then uses the WriteEntityChunks API to embed the downloaded JavaScript into the HTML content of the response. It then returns the altered response to redirect the user to the destination intended by the actor. Figure 26. Injecting JavaScript code to response data. Figure 27. Fetching JavaScript code from C2 server. BadIIS retrieves malicious JavaScript code from a C2 server and redirects users to malicious websites instead of legitimate ones. By not embedding the JavaScript code directly in the binary, it allows easier modification of the redirect targets and helps evade detection by antivirus security products. The script is programmed to show a brief loading message before automatically redirecting the user to a malicious site. The redirect function and alert message vary across different C2 servers; some scripts reference two

C2 servers and randomly select one with a 50% probability. Additionally, the alert message language is tailored to match the target region of the user. Figure 28. JavaScript code with alert message in Portuguese. Figure 29. Two different
C2 servers in JavaScript code. The second cluster of the new BadIIS malware also includes handlers named CHttpModule
::OnBeginRequest and CHttpModule
::OnSendResponse . In this cluster, OnBeginRequest is used as a decision point to execute before any intensive processing occurs, while OnSendResponse handles output modification to ensure that no other module can override the redirect. This cluster also features three modes: SEO fraud mode, injector mode and
proxy mode. Notably, the injector and
proxy modes operate under the SEO fraud mode umbrella, which itself has four variants tailored to different scenarios: All interface hijacking targets all webpages on the webserver, replacing original content for both search engine crawlers and users. Figure 30. All interface hijacking. Homepage hijacking targets only the homepage, substituting its content for search engine crawlers and users. Figure 31. Homepage hijacking. Global reverse proxy configures a
proxy to automatically
replace
content for search engine crawlers and users. Figure 32. Global reverse proxy. Specify
URL
path reverse
proxy configures a
proxy to automatically
replace
content for search engine crawlers and users. Figure 33. Specify
URL
path reverse
proxy. The
URL
path pattern referred to as Tezhengma in the debug strings by the actor includes multiple versions. Some of these versions partially match the patterns found in the first cluster of BadIIS malware. xxm
|dabo
|lingdu

|images cash
|bet
|gambling
|betting
|casino
|fishing
|deposit
|bonus news
|cash
|bet
|gambling
|betting
|casino
|fishing
|deposit
|bonus
|sitemap news
|cash
|bet
|gambling
|betting
|casino
|fishing
|deposit
|bonus
|sitemap
|app
|ios
|video
|games
|xoso
|dabong
|nohu app
|news
|ios
|android
|cash
|bet
|gambling

```
|betting
|casino
|fishing
|deposit
|bonus
|sitemap
|qsj
|rna
|muv
|zop
|vna
|apk
|hots
|cocs
|mohu
|banc
```

The injector mode injects JavaScript in each SEO fraud type when the user-agent and referer do not match its criteria. The algorithm is same as the first cluster BadIIS; it verifies the user-agent to identify search engine crawlers and checks the referer to determine if the user is browsing from an expected source. User-agent Referer Baiduspider Sogouspider Sogou web spider 360spider YisouSpider Googlebot Bingbot BingPreview MicrosoftPreview baidu sogou sm [.] cn 360 so[.]com toutiao google bing Table 4. Combination of User-Agent and Referer headers used for injecting JavaScript to redirect the browser. Coverage Ways our customers can detect and block this threat are listed below. Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here. Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here . Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual , Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat. Cisco Secure Network/
Cloud Analytics (Stealthwatch/Stealthwatch

Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device. Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products. Cisco Secure Access is a modern cloud-delivered Security Service Edge (SSE) built on Zero Trust principles. Secure Access provides seamless transparent and secure access to the internet, cloud services or private application no matter where your users work. Please contact your Cisco account representative or authorized partner if you are interested in a free trial of Cisco Secure Access. Umbrella , Cisco s secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them. Additional protections with context to your specific environment and threat data are available from the Firewall Management Center . Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network. Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org . Snort SIDs for the threats are: 65346, 65345 ClamAV detections are also available for this threat: Win.Malware.SysShell-10058032-0 Win.Malware.NewBadIIS-10058033-0 Win.Malware.BadIISCR45-10058034-0 Win.Malware.WebShellCn-10058035-0 Win.Packed.CSBeaconCn-10058036-0 Indicators of compromise (IOCs) The IOCs can also be found in our GitHub repository here .